高等学校计算机专业教材精选·网络与通信技术

网络安全基础教程

许 伟 廖明武 等编著



清华大学出版社

网络安全基础教程

许伟　廖明武 等编著

清华大学出版社
北　京

内 容 简 介

本书详细介绍了网络安全的基础知识与典型应用，共分为 9 章，主要内容包括网络安全概论、计算机病毒防范、数据加密、防火墙技术、计算机安全管理、局域网安全管理、广域网安全管理、网络安全规划和网络安全实施。在每一章中，不仅讲解了基本原理，还尽量让读者能够动手操作一些实践项目，让读者有思考和练习的空间。

本书在编写过程中，介绍了实用的和最新的技术，做到通俗易懂、图文并茂；并且本书采用循序渐进的方式，结合实际案例，有助于读者上机练习。

本书可作为大专院校相关课程教材，也可作为网络安全爱好者的自学参考书。

图书在版编目（CIP）数据

网络安全基础教程 / 许伟，廖明武等编著. —北京：清华大学出版社，2009.6
（高等学校计算机专业教材精选·网络与通信技术）
ISBN 978-7-302-19312-8

I. 网… II. ①许…②廖… III. 计算机网络－安全技术－高等学校－教材
IV. TP393.08

中国版本图书馆 CIP 数据核字（2009）第 008761 号

责任编辑：战晓雷　王冰飞
责任校对：梁毅
封面印制：
出版发行：清华大学出版社　　**地　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编：**100084
社　总　机：010-62770175　　**邮　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　销：全国新华书店
开　本：185×260　**印　张：**19.5　**字数：**483 千字
版　次：2009 年 6 月第 1 版　**印　次：**2009 年 6 月第 1 次印刷
印　数：1~
定　价：　.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：（010）62770177 转 3103　　产品编号：

前　　言

垄徯助蓋羭缸禚佶争，味袨味叀展诽箪杸蓋偪趱惘晁眦壶徖，跦柁跦奶蓋攸垄俛嶙Internet，来价攸逴觝屦勹淨囙、佘莽乪逸磅幁佤竖限蓋诽箪杸睮逺搁，谔奶攸蓋诽箪杸争宴億暱减仪了攸、淨呔當艏至佘杸九蓋鈩觝倧惋，拔佁，羭缸寥凄帿缫扬三乜了晁眦鈩觝蓋豚眙。撥至肤鄂貌桁岜（Federal Bureau of Investigation，FBI）持咦嗂祼，反小惘羭缸寥凄斗剗旌敘垄遬廐书膐。诽箪杸斗剗蓋担斿佁否展羭缸哨展逸磅谛陊偪趱磅异蓋乩昉壶閹，借扬伒展黗姞階烇垚哨蚶挻砉嶙羭（VPN）箥絅瓴静沛蓋壶閹。周梓，亻借扬伒禚佶展羭缸寥凄砉叀攸唊蓋静沛，味稍缠缣静觝醻奤賨妏瓴篕搸搽寥凄迋佒乪魄佒蓋砉叀攸唊。

扭垩诽箪杸寥凄階捓賨勦岢乩吭通，斛廸、佝叀圾侯哨了攸诽箪杸嶙抓蓋寥凄慫谢酙乩徖，诽箪杸忤尕景吳劆凡鄻竟趏、诽箪杸瘖氮哨羭缸尉对蓋斗剗，逺价斗剗応応溧来柝妃蓋餪雅惘。鈩觝旌揊、旣佒蓋穎嶙、浲覞、乾妍哨複眳，乩侟佶缵至佘、佝叀哨了攸遼扬幄妃蓋缫涪搔妍，聯买乾鈩反否劆至佘寥凄哨禚佶穿寶。姞侱倹捓诽箪杸争蓋倧惋乩複鞓洱萓吲、眳嶙、箣爛哨碕垫，帿扬三侣攸减净哨任忡詤乞蓋陊眙。

逭廐柁，扭佈展仪羭缸哨倧惋寥凄昕韡乩瞀泽来佤三，廳豁豐来减鄻附、砉叀淨呔哨砉叀攸奇亻拱涑伒迟妃蓋級勦展伴逺糗陊眙，亻詤乞伒忤奶陊眙。侢瞀，羭缸寥凄瞀乜了乩昉吳卲吭岱蓋飢逹，羭缸斗剗哨階澾垄乩昉蓋厶彤争。跓剹，垄 20 皊缆 90 廐佨，倧惋寥凄陊眙岂觝佁箓厵瘖氮蓋黴彫剖玪，郿晒瘖氮蓋吳卲、伃嗟哨佼擢瞀罯憾蓋。呪柁，逷涑 21 皊缆呪，霏暱伮肤羭嶙抓蓋壶閹，伮肤羭佁否佤三遗遶嶙厫谊蓋 TCP/IP 複廛浧搁缏，逺岍三跦柁跦奶蓋斗剗佼擢遭忠搬偲伒佤嶙廄呌。逺乩侟伃嗟伒展材奶材徖妃蓋階忽杸劒蓋静沛，周晒亻睮廳搬偲伒涑們展眙哨涑們聡。岍階瘖氮伃叀聯設，逺稍率趪漾扫連磅显搬餔伒斗剗幁溧，亻搬餔伒階忽幁溧蓋畣枞惘沐廐。伮肤羭蓋曊炞犸惘亻俛遗吳三乜了溧来忤奶睊档蓋琋壟，聯买察逴三斗剗聡搬偲伒萱廎呋佁吭跓斗剗蓋垌昕。垄寥凄助礋爛吳蓋周晒，坐缙寥凄岱彝蓋谄谖豚眙亻垄吭岱哨吳卲。

伷霏暱羭缸哨倧惋寥凄逺飕伃叀蓋扬爑，扭佈殿垄睊譬逺了橀惼寨凄哨柖柒书複淨彝。味淨呔殿垄遬毀搬餔寥凄慫谢哨展寥凄夫勼蓋嗟廳。氰姞豐惂迋淨呔，柁缫乜异疍仪伲佈蓋寥凄猒刑聯複攸佈嚎箅，玪垄，伲佈帿缫瞀寥凄嗟廳书暄殿蓋寃黼。玪垄惂迋蓋伃唝垄吭幟产呪，佶乩昉垌搬偲铤展寥凄陊眙蓋裁九。

柒仂谬缢伧缩伒倧惋寥凄飢逹蓋味了昕韡，岂觝凡尕来：羭缸寥凄橀谖、诽箪杸瘖氮階荟、旌揊匇九、階烇垚拜枋、诽箪杸寥凄篰瑢、岜逹羭寥凄篰瑢、廛逹羭寥凄篰瑢、羭缸寥凄訠剾哨羭缸寥凄寺昙。垄氩乜笼争，乩侟谎詤伒埰柒叻瑢，逴歽敘谇缟愿聡勾抧攮佤飕睊，谅愿聡来恹智哨缟亼蓋竖限。

柒仂溧来寨貉蓋砼谢侯絅，展砼谢蓋谎詤缢艘谬歽，怆廯棃逷，遶傳景戞，賨遬毀搬餔愿聡蓋俛嶙賨勦，幅垩寂亼拜賨。

吕韡，柒仂净鈩寺蹑、徖貌寺嶙。氩笼豚呪蓋缟亼眙，疍箓厵劆畣枞，寨凄幫眲伒豁笼淥否蓋鈩觝砼谢。

柒仂亗觝韡呭嶦杷仢訑羚缸寥凄堜矽砼谢盠戅聡。蛙焚柒仂晵乜柒堜矽仂，偁觝沞戅聡晵燻缟盠诽箽枤疄抓，缫应侥疄诽箽枤幁叵抮寂亼，腙妏燻缟侥疄疑宬鄊侠哨 Web 涫誸嚁，仢訑堜柒盠枋豉。戅聡廰豁凓奣堜柒盠诽箽枤砼谢，偁乩靜觝絧瓺寂亼诽箽枤乴叀盠豚稹。

柒仂亘渪厔妃寂谔佻、弰唤瞉聝幣亗署，枪臚哨珧靓厶奇亻 呑匇仢署凵哨偊爛。呑匇柒仂署凵幁叵盠逴来枪佻、酉混、刋锫、䪼氡、髈佁迴、郯磖、郯刽廄、哄伋、蒿瞉、鄭嗼蔫、隫尒凷、傆浏暧、鼠蛸、呱幃琩、襤蕢、鍪飲、珧噥俏、咐象佻、寧霊、俍嗼剟、民混、髈亙媂、酉稪、柃嗼柳、隫礦、枪象镧、剀归凷、剀宬璥、忬荍瞉、鮫寚、跑逸镧篓伖。

柒仂垄署凵連稹争，呑聍仢谔奶乪羚缸寥凄砼谢睔减盠枞悅哨仂粩，展仪逵价既笼盠叵聡哨仂粩署聡垄毀衎祼褫怟盠惓豟！羚缸寥凄柒輇晵乜了昌湮盠夫狂，谔奶盠瑢谖、寺踂仪垄掑緎产争，凩匇书署聡寂谢来隬抮署凵盠痫潫，姑宴垄镵登哨乩威产奠，黗戅聡拕说捣殿。

叵　聡
2009 庣 2 枂

目　　录

第 1 章　网络安全概论 1
1.1　计算机网络的发展和应用 1
1.2　网络安全所面临的挑战 2
　1.2.1　网络内部安全挑战 2
　1.2.2　网络外部安全挑战 3
1.3　网络安全的内容 3
　1.3.1　计算机安全 4
　1.3.2　局域网安全 5
　1.3.3　广域网安全 6
1.4　网络安全问题的解决思路 7
　1.4.1　技术角度 7
　1.4.2　管理角度 9
1.5　网络安全的重要性 9
1.6　网络安全的紧迫性 10
习题 11

第 2 章　计算机病毒防范 12
2.1　计算机病毒的基本概念 12
　2.1.1　什么是计算机病毒 12
　2.1.2　计算机病毒的命名 13
　2.1.3　计算机病毒的分类 14
2.2　计算机病毒的特点及表现现象 15
　2.2.1　计算机病毒的特点 16
　2.2.2　计算机病毒发作前的表现现象 19
　2.2.3　计算机病毒发作时的表现现象 21
　2.2.4　计算机病毒发作后的表现现象 22
2.3　计算机病毒检测方法 23
　2.3.1　手动检测病毒的常用辅助工具 24
　2.3.2　手动清除飘雪病毒 29
2.4　计算机病毒防范措施 32
　2.4.1　计算机病毒的预防 32
　2.4.2　计算机病毒感染后的一般修复处理方法 34
　2.4.3　诺顿杀毒软件 35
习题 39

第 3 章　数据加密 40

3.1 数据加密概述 40
3.1.1 数据加密 40
3.1.2 基本概念 42
3.2 对称加密算法 46
3.2.1 DES 算法及其基本思想 47
3.2.2 DES 算法的安全性分析 49
3.2.3 DES 加密算法举例 50
3.3 公开密钥算法 52
3.3.1 RSA 算法及其基本思想 52
3.3.2 RSA 算法的安全性分析 53
3.3.3 RSA 加密算法举例 54
3.4 数据加密技术的应用 57
3.4.1 数据加密 57
3.4.2 传输安全 59
3.4.3 身份认证 59
3.4.4 在电子商务方面的应用 61
3.4.5 加密技术在 VPN 中的应用 61
3.5 加密举例 61
习题 64
第 4 章 防火墙技术 65
4.1 防火墙基本概念 65
4.1.1 防火墙定义 65
4.1.2 防火墙的功能 66
4.1.3 防火墙的分类 67
4.1.4 防火墙体系结构及组合形式 71
4.2 用协议分析工具学习 TCP/IP 74
4.2.1 试验环境 75
4.2.2 测试过程 75
4.2.3 过程分析 77
4.2.4 实例分析 80
4.3 包过滤防火墙 88
4.3.1 包过滤防火墙的一般概念 88
4.3.2 包过滤防火墙的工作原理 89
4.3.3 包过滤器操作的基本过程 90
4.3.4 包过滤技术的优缺点 90
4.4 代理防火墙 91
4.4.1 为什么要进行代理 91
4.4.2 代理服务的优缺点 92
4.4.3 代理服务的工作方法 93

4.4.4 代理服务器的使用 94
4.5 防火墙技术的发展趋势 95
4.5.1 防火墙包过滤技术发展趋势 95
4.5.2 防火墙的体系结构发展趋势 95
4.5.3 防火墙的系统管理发展趋势 96
4.6 防火墙应用 97
习题 101
第 5 章 计算机安全管理 102
5.1 软件安全 102
5.1.1 系统补丁 102
5.1.2 配置管理 108
5.1.3 系统备份 116
5.1.4 反间谍软件 123
5.2 数据安全 128
5.2.1 文件管理 128
5.2.2 接口管理 129
5.2.3 打印管理 130
5.2.4 用户管理 131
5.2.5 数据备份 139
习题 143
第 6 章 局域网安全管理 144
6.1 局域网概述 144
6.1.1 网络概况 145
6.1.2 网络应用 146
6.1.3 网络结构特点 147
6.2 安全评估 147
6.2.1 网络安全为何会失败 147
6.2.2 为何要执行安全评估 149
6.2.3 规划安全评估 149
6.2.4 安全评估范围 150
6.2.5 安全评估目标 150
6.2.6 安全评估的类型 150
6.2.7 使用漏洞扫描来评估网络安全 151
6.2.8 使用突破测试来评估网络安全 151
6.2.9 安全审核的组成部分 152
6.2.10 报告安全评估结果 152
6.3 网络系统安全风险分析 152
6.3.1 物理安全风险分析 153

6.3.2 网络平台的安全风险分析 153
6.3.3 系统的安全风险分析 153
6.3.4 应用的安全风险分析 154
6.3.5 管理的安全风险分析 154
6.3.6 黑客攻击 154
6.3.7 通用网关接口（CGI）漏洞 155
6.3.8 恶意代码 155
6.3.9 病毒的攻击 155
6.3.10 人员的安全风险分析 155
6.3.11 网络的攻击手段 156
6.4 安全需求与安全目标 157
6.4.1 安全需求分析 157
6.4.2 网络安全策略 158
6.4.3 系统安全目标 158
6.5 网络安全方案总体设计 158
6.5.1 安全方案设计原则 158
6.5.2 安全服务、安全机制与安全技术 159
6.6 网络安全体系结构 160
6.6.1 物理安全 160
6.6.2 网络安全 160
6.6.3 系统安全 163
6.6.4 信息安全 163
6.6.5 应用安全 164
6.6.6 管理安全 164
6.6.7 用户安全 166
6.6.8 安全审计 166
6.7 网络安全技术 167
6.7.1 桌面管理 167
6.7.2 网络管理 170
6.6.3 网络监控审计 175
6.8 网络安全服务 179
6.8.1 借用安全评估服务帮助我们了解自身安全性 179
6.8.2 采用安全加固服务来增强信息系统的自身安全性 182
6.8.3 部署专用安全系统和设备提升安全保护等级 182
6.8.4 加强安全教育培训来减少和避免安全事件的发生 182
6.8.5 引入应急响应服务及时有效地处理重大安全事件 183
6.8.6 借助安全通告服务对安全威胁提前预警 183
6.9 操作案例 183
6.9.1 通过配置来增强系统安全性 184

6.9.2　计算机外设管理 188
6.9.3　局域网资产管理 191
习题 195

第 7 章　广域网安全管理 196
7.1　广域网的风险 196
7.2　防火墙技术应用 197
7.2.1　防火墙部署 197
7.2.2　防火墙的配置 200
7.3　VPN 技术 203
7.3.1　VPN 基础 204
7.3.2　部署 VPN 208
7.4　安全审计 213
7.5　企业广域网安全 214
7.6　电子商务安全 216
7.6.1　电子商务安全策略 216
7.6.2　电子商务安全技术 218
7.6.3　电子商务安全规范 220
7.6.4　Windows 2000 的安全机制 221
7.6.5　Windows 2000 下建立 CA 中心的具体操作过程 222
7.7　电子政务安全 225
习题 232

第 8 章　网络安全规划 233
8.1　网络和应用现状分析 233
8.1.1　网络中存在的安全威胁 233
8.1.2　网络现状分析 234
8.1.3　应用现状分析 235
8.1.4　安全系统设计目标 235
8.2　网络安全系统整体规划 236
8.2.1　安全体系框架分析 237
8.2.2　安全子系统划分 239
8.3　通信平台安全子系统 239
8.4　网络平台安全子系统 240
8.4.1　网络平台安全域划分 240
8.4.2　网络平台安全需求分析 240
8.4.3　安全网络拓扑结构 241
8.4.4　防火墙配置方案 241
8.4.5　总部局域网防火墙配置方案 241
8.4.6　入侵检测系统设计 242

8.4.7 网络平台安全子系统小结......243
8.5 系统平台安全子系统......243
8.5.1 系统平台安全需求分析......243
8.5.2 系统平台安全域的划分......243
8.5.3 服务器安全配置......244
8.5.4 漏洞扫描和评估系统......246
8.5.5 企业防病毒体系......247
8.6 应用平台安全子系统......248
8.6.1 安全管理对象和安全域划分......249
8.6.2 应用平台安全子系统设计思路......250
8.6.3 应用系统安全机制分析......250
8.6.4 应用系统安全风险分析......251
8.6.5 应用安全平台需求分析......252
8.7 网络安全规划案例......253
8.7.1 背景简介......253
8.7.2 评估结果......254
8.7.3 安全计划......256
8.7.4 资源和预算......257
8.8 安全服务......258
习题......262
第 9 章 网络安全实施......263
9.1 网络安全实施原则......263
9.1.1 网络安全策略......264
9.1.2 网络安全分步实施......266
9.2 安全性设计过程......269
9.2.1 安全原则......270
9.2.2 监视和控制......272
9.3 网络安全措施......273
9.3.1 容易的工作......273
9.3.2 较难的任务......278
9.3.3 请求帮助......279
9.4 保护网络安全的 7 个步骤......281
9.4.1 保护你的台式机和便携机......282
9.4.2 保证数据安全......282
9.4.3 安全地使用 Internet......283
9.4.4 保护网络......284
9.4.5 保护服务器......286
9.4.6 保护业务应用程序......287
9.4.7 从服务器管理台式机或便携机......288

9.5 及时备份数据 289
9.6 保护敏感文档 291
9.7 日志分析 292
习题 294

第 1 章　网络安全概论

教学提示

计算机网络的广泛应用，为人们的生产、生活、工作、娱乐等带来了方便，同时由于技术原因和人为因素，也为人们带来了诸多安全隐患。

本章首先回顾了计算机网络技术的发展和应用情况，然后提出当前网络安全所面临的挑战，并对网络安全所涉及的内容进行了简要说明，提出了解决网络安全问题的总体思路，最后强调了网络安全的重要性和紧迫性。

通过对本章的学习，应当对网络安全问题以及解决网络安全问题的方法有一个初步的认识，为进一步学习相关知识奠定一个良好的基础，并认清做好网络安全工作的重要意义。

教学重点

- 理解网络安全所面临的挑战。
- 掌握网络安全的内容。
- 掌握网络安全问题的解决思路。
- 理解网络安全的重要性和紧迫性。

1.1　计算机网络的发展和应用

计算机技术与通信技术相结合，使计算机网络技术得以产生和发展。

1．网络技术的发展

最初的计算机网络是一台主机通过导线连接若干个远程的终端，这种网络称为面向终端的计算机通信网。它是以单个主机为中心的星形网，效率不高，功能有限。这就是第一代网络。

1969 年 12 月在美国诞生了阿帕网络（ARPANET），它以通信子网为中心，许多主机和终端设备在通信子网的外围构成一个用户资源子网，通信子网不再使用电话通信的电路交换方式，而采用了数据通信的分组交换方式，大大提高了通信效率，降低了通信费用。这就是第二代计算机网络。

国际标准化组织（ISO）于 1977 年提出了著名的开放系统互连参考模型，简称 OSI/RM，从此以后，就开成了第三代计算机网络，其中，最引人注目的就是 Internet 的飞速发展。

进入 20 世纪 90 年代，计算机网络的发展更加迅速，出现了宽带综合业务数字网（B-ISDN），这就是第四代计算机网络。

我国在 1989 年建成第一个用于数据通信的公用分组交换网，1993 年建成新的覆盖全国的中国公用分组交换网（CHINAPAC），同年 3 月，我国启动金桥工程、金卡工程、金关工程等一系列“金”字工程，计算机网络是这些工程中的重要组成部分。1995 年邮电部投资建成中国公用计算机互联网（CHINANET），提供 Internet 业务。

2. 网络技术的应用

计算机网络通常应用于以下几个方面。

1）数据通信

它使分布在不同位置的计算机与计算机可以进行通信，互相传送数据，方便地进行信息交换。例如，使用电子邮件、视频会议等。

2）资源共享

这是计算机网络最具有吸引力的功能，在网络范围内，用户可以共享软件、硬件、数据等资源，而不必考虑用户以及资源所在的位置。

3）实现分布式计算

由于有了计算机网络，许多大型信息处理问题可以借助于分散在网络中的多台计算机协同完成，解决单机无法完成的信息处理任务。特别是分布式数据库管理系统，它使分散存储在网络不同系统中的数据，使用时好像集中存储和集中管理那样方便。

4）提高计算机系统的可靠性和可用性

网络中的计算机可以互为后备，一旦某台计算机出现故障，它的任务可由网中其他计算机取而代之。当网中计算机负荷过重时，网络可将新任务分配给较空闲的计算机去完成，提高了每台计算机的可用性。

1.2 网络安全所面临的挑战

计算机网络的出现，从很大程度上改变了人们进行信息交流的方式，以前需要大量书信用很长时间才能解决的问题，今天可以通过电子信息来迅速解决，不但大大降低了成本，而且效率得到了很大的提高。当然，计算机网络在带给方便、高效的同时，也存在一定程度上的安全问题，需要认真对待，否则，我们可能会蒙受各种程度的损失。

1.2.1 网络内部安全挑战

网络内部安全挑战是指内部人员因工作需要或者外部人员因有机会直接在一个特定网络内部进行操作而造成的安全威胁。

1. 网络硬件安全挑战

网络硬件安全挑战是指因为计算机网络的硬件设备故障所造成的安全问题。网络硬件设备是计算机网络正常使用的基础，要让计算机网络正常、稳定、高效运行，那么合理选择硬件设备、合理规划并搭建网络系统、正确配置运行参数都是必不可少的。好在随着计算机技术和网络技术的不断发展和进步，计算机网络硬件设备本身的稳定性和可靠性都有了很大程度的提高，发生故障的几率已经很小了，目前的挑战主要是如何合理规划并搭建网络以及正确配置网络硬件的运行参数了，这两项对于一个大型的网络系统是至关重要的。

2. 网络软件安全挑战

网络软件安全挑战是指系统中所安装和使用的软件没能提供预定功能或者提供了错误的功能。其中最明显的例子就是操作系统，操作系统应该提供一个安全的操作环境，因为各个方面的原因可能使操作系统存在各种各样的漏洞。同样数据库系统也是一样，可能因

为考虑不周而出现漏洞，使得原本安全的系统变得不安全了。

病毒程序和木马程序通常是附在正常的程序或者文件之中进行传播，它们所提供的功能是客户所不需要的，属于错误的功能。

3．人为安全挑战

人为安全挑战分为两种类型，第一种是无意造成的安全威胁，第二种是有意造成的安全威胁。两者的操作结果都是因出现了错误的操作而导致不希望的后果，但前者不是操作者本意的表示，比如操作者不小心误操作将自己计算机或者文件服务器上的文件删除了。而后者正好是操作者本意的表示，比如离职的职员出于对公司的不满，将自己计算机或者其他计算机上的有用文件删除了。

这两种情况虽然结果是一样的，但是性质却是完全不同的。对于无意造成的安全威胁相对比较容易解决，而对于有意造成的安全威胁需要采取多种措施才能有较好的效果，这将是本书在后面将要讨论的话题。

1.2.2　网络外部安全挑战

网络外部安全挑战是指来自外部网络（外部网络是指除了用户可控的局部网络以外的网络，如 Internet 网）的安全威胁，包括两种情况，一种是在使用网络服务时引入的安全问题，因为只有在连接网络并使用网络服务时才会发生，所以称为被动攻击，如下载文件资料时引入病毒、木马等有害程序；另一种是来自外部的黑客攻击，因为只要和外部网络处于连接状态，即使没有进行任何操作仍然可能受到攻击，所以称为主动攻击，即利用系统安全漏洞非法进入计算机系统进行非法操作，如破坏系统资源或者窃取资料。

1．被动攻击

被动攻击的特点是目标性不明确，在攻击发生之前并没有确定某个具体的计算机为目标，只是把有害程序放置在一个特定的位置，通常是一个网站上，当访问者访问网页时，如果访问者的计算机安全性不够高的话，有害程序就会直接下载到访问者的计算机上，并在适当的时候被激活，从而对访问者计算机进行非法操作。也有的将有害程序放置在网页上，然后引诱访问者去点击，从而将有害程序下载到访问者的计算机上。还有将有害程序藏匿在资料文件中，等访问者下载资料文件的同时将有害程序一起下载。

2．主动攻击

主动攻击的特点是具有明确的目标，通常使用的方式是通过扫描工具对某个特定的网络范围进行扫描，对扫描得到的计算机再逐个进行试探性攻击，找出安全性比较弱的计算机进行攻击，从而达到破坏目标计算机系统或窃取目标计算机上资料的目的。

1.3　网络安全的内容

网络安全主要包括三个方面的内容，即计算机安全、局域网安全以及广域网安全。计算机是网络中的一个非常重要的组成部分，其负责存储、计算、发送以及接收数据信息，所以保证计算机的安全是网络安全的一个重点。除了要保证单台计算机的安全，还要考虑整个网络系统的安全，对于一个网络系统，通常是一个完整的系统，其中某些部分出现问题，可能会危及整个网络系统的安全运行。对于 Internet 网的使用也存在多种网络安全问题，

需要我们在使用之前做好安全防范工作，将网络安全风险减小到最低。

1.3.1 计算机安全

计算机安全是指单台计算机范围内的安全，通常包括系统安全和数据安全两个方面，系统安全是基础，数据安全是目的。这是网络安全最基本的内容，没有计算机范围内的安全，也就不可能有网络范围的安全。

1. 系统安全

系统安全是指计算机系统能够正常、稳定、高效地提供其功能。系统安全的问题来自多个方面，可能是病毒、木马程序、黑客攻击、人为破坏、硬件故障等。具体体现在以下几个方面。

（1）补丁安全。通常的操作系统和其他系统软件都容易出现安全漏洞，给病毒、木马程序、黑客等以可乘之机，注意随时对系统进行升级并尽可能安装最新的补丁程序是防止安全漏洞被利用的最有效方法。

（2）配置安全。包括系统中账户的建立、密码的设置、注册表访问权限的控制、控制面板访问权限的管理以及文件系统的安全配置等，通过对系统自身的安全系统进行合理的配置，可以大大提高系统的安全性。

（3）系统备份。系统的安全威胁是来自多个方面的，只要一个方面没有考虑到就可能影响系统的正常运行，甚至使系统停止运行。如果重新配置系统需要很长的时间，最有效的方法就是有计划地对系统进行备份，在必要的时候通过恢复备份的方式来解决系统问题。

（4）杀毒。计算机病毒和木马程序是威胁计算机系统安全的两个至关重要的因素，因为病毒和木马程序通常都是隐藏在后台，不易被发现，只有遭到破坏以后才会被发现，而且两者的破坏性都可能很大，所以对病毒和木马程序的防范决不能掉以轻心。

2. 数据安全

数据安全是指用户存储在计算机上的数据信息不被非法查看、修改、移动和删除。数据安全威胁主要来自三个方面，一方面是系统安全被突破以后带来的数据安全威胁；第二方面是人为操作带来的数据安全威胁，第三方面是硬件故障带来的数据安全威胁。要做好数据安全工作，必须同时注意到这三个方面的威胁。具体体现在以下几个方面。

（1）文件安全。对计算机上的文件操作进行监控审计，对文件操作进行记录，并对必要的文件提供自动备份和恢复的功能，以便审计时及时发现和找出非法文件操作的原因，及时采取措施防止非法的文件操作造成文件资料的泄密、破坏，提高文件安全性。

（2）外设接口安全。计算机提供多种接口是为了使用上的方便，但是如果没有合理的规划和管理，这些接口可能成为数据安全的一大隐患。特别是具有将计算机上的数据拷贝带出的接口，如软驱、刻录机、打印机、USB 接口的存储设备等。

（3）打印安全。打印文件是日常工作和生活中常见的一件事情，但是如果有人将不应该打印的重要文件资料打印出来带到不应该带去的地方就麻烦了，比如软件源代码、工程项目文件、客户资料等。

（4）刻录安全。刻录光盘是一种常用的系统备份或者数据备份方式，最重要的原因是该方式简单，而且成本很低。但是如果没有合理的管理，可能导致非法将计算机中的文件进行刻录，从而导致信息泄密。

（5）操作安全。自己和别人在操作计算机时都可能存在误操作的情况，而且在别人操作自己计算机时，并不能保证所进行的操作都是完全合乎自己意愿的，所以需要使用一些监控功能，一方面监视操作过程，另一方面防止操作者进行非法操作。

1.3.2　局域网安全

局域网安全实际上就是计算机安全再加上局域网内计算机直接的相互安全影响。局域网安全可以从以下几个方面来理解。

（1）网络物理安全。网络的物理安全主要是指地震、水灾、火灾等环境事故，电源故障，人为操作失误或错误，设备被盗、被毁，电磁干扰，线路截获，以及高可用性的硬件、双机多冗余的设计、机房环境及报警系统、安全意识等。它是整个网络系统安全的前提，制定健全的安全管理制度，做好备份，并且加强网络设备和机房的管理，这些风险是可以避免的。

（2）网络平台安全。网络结构的安全涉及到网络拓扑结构、网络路由状况及网络的环境等。安全的应用往往是建立在网络系统之上的，网络系统的成熟与否直接影响安全系统成功的建设。

（3）系统安全。所谓系统的安全显而易见是指整个局域网网络操作系统、网络硬件平台是否可靠且值得信任。 没有完全安全的操作系统，但是，我们可以通过对操作平台进行安全配置，对操作和访问权限进行严格控制，来提高系统的安全性，不但要选用尽可能可靠的操作系统和硬件平台，而且必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性。其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

（4）应用安全。应用系统的安全跟具体的应用有关，它涉及很多方面。应用系统的安全是动态的、不断变化的，应用的安全性也涉及到信息的安全性，它包括很多方面。应用的安全性涉及到信息、数据的安全性，信息的安全性涉及到机密信息泄露、未经授权的访问、破坏信息完整性、假冒、破坏系统的可用性等。对于有些特别重要的信息需要对内部进行保密的（比如领导子网、财务系统传递的重要信息），可以考虑在应用级进行加密，针对具体的应用直接在应用系统开发时进行加密。

（5）管理安全。管理是网络安全中最重要的部分。责权不明，管理混乱、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。责权不明，管理混乱，使得一些员工或管理员随便让一些非本地员工甚至外来人员进入机房重地，或者员工有意无意泄露他们所知道的一些重要信息，而管理上却没有相应制度来约束。建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是管理制度和管理解决方案的结合。

（6）不满的内部员工。不满的内部员工可能在 WWW 站点上开些小玩笑，甚至搞破坏。不论如何，他们最熟悉服务器、小程序、脚本和系统的弱点。对于已经离职的不满员工，可以通过定期改变口令和删除系统记录以减少这类风险。但还有心怀不满的在职员工，这些员工比已经离开的员工能造成更大的损失，例如他们可以传出至关重要的信息、泄露安全重要信息、错误地进入数据库、删除数据等等。

1.3.3 广域网安全

广域网安全是指因使用建立在 Internet 网基础上的服务而造成的安全威胁。使用的 Internet 服务是指使用网络上其他计算机所提供的服务或者向其他计算机提供服务，如电子邮件、WWW 服务、FTP 服务、点对点通信。

1. 公开服务器面临的威胁

公开服务器（WWW、EMAIL 等服务器）作为对外信息发布平台，一旦不能运行或者受到攻击，对企业的声誉影响巨大。同时公开服务器本身要为外界服务，必须开放相应的服务；每天，黑客都在试图闯入 Internet 节点，这些节点如果不保持警惕，可能连黑客怎么闯入的都不知道，甚至会成为黑客入侵其他站点的跳板。因此，规模比较大的网络管理人员对 Internet 安全事故做出有效反应变得十分重要。我们有必要将公开服务器、内部网络与外部网络进行隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他请求服务在到达主机之前就应该遭到拒绝。

2. 黑客攻击

黑客们的攻击行动是无时无刻不在进行的，而且会利用系统和管理上的一切可能利用的漏洞。公开服务器存在漏洞的一个典型例证，是黑客可以轻易地骗过公开服务器软件，得到 UNIX 的口令文件并将之送回。黑客侵入 UNIX 服务器后，有可能修改特权，从普通用户变为高级用户，一旦成功，黑客可以直接进入口令文件。黑客还能开发欺骗程序，将其装入 UNIX 服务器中，用以监听登录会话。当它发现有用户登录时，便开始存储一个文件，这样黑客就拥有了他人的账户和口令。这时为了防止黑客，需要设置公开服务器，使得它不离开自己的空间而进入另外的目录。另外，还应设置组特权，不允许任何使用公开服务器的人访问 WWW 页面文件以外的东西。在这个企业的局域网内我们可以综合采用防火墙技术、Web 页面保护技术、入侵检测技术、安全评估技术来保护网络内的信息资源，防止黑客攻击。

3. 通用网关接口（CGI）漏洞

有一类风险涉及通用网关接口（CGI）脚本。许多页面文件和指向其他页面或站点的超链接。然而有些站点用到这些超链接所指站点寻找特定信息。搜索引擎是通过 CGI 脚本执行的方式实现的。黑客可以修改这些 CGI 脚本以执行他们的非法任务。通常，这些 CGI 脚本只能在这些所指 WWW 服务器中寻找，但如果进行一些修改，他们就可以在 WWW 服务器之外进行寻找。要防止这类问题发生，应将这些 CGI 脚本设置为较低级用户特权。提高系统的抗破坏能力，提高服务器备份与恢复能力，提高站点内容的防篡改与自动修复能力。

4. 恶意代码

恶意代码不限于病毒，还包括蠕虫、特洛伊木马、逻辑炸弹和其他未经同意的软件。应该加强对恶意代码的检测。

5. 病毒的攻击

计算机病毒一直是计算机安全的主要威胁。能在 Internet 上传播的新型病毒，例如通过 E-mail 传播的病毒，增加了这种威胁的程度。病毒的种类和传染方式也在增加，国际空间的病毒总数已达上万甚至更多。当然，查看文档、浏览图像或在 Web 上填表都不用担心病

毒感染，然而，下载可执行文件和接收来历不明的 E-mail 文件需要特别警惕，否则很容易使系统导致严重的破坏。典型的 CIH 病毒就是一可怕的例子。

6．网络的攻击手段

一般认为，目前对网络的攻击手段主要表现在以下几个方面。

非授权访问：没有预先经过同意，就使用网络或计算机资源被看作非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

信息泄露或丢失：指敏感数据在有意或无意中被泄露出去或丢失，它通常包括，信息在传输中丢失或泄露（如黑客利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账号等重要信息。），信息在存储介质中丢失或泄露，通过建立隐蔽隧道等窃取敏感信息等。

破坏数据完整性：以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。

拒绝服务攻击：它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

利用网络传播病毒：通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

1.4　网络安全问题的解决思路

网络安全问题是一个相当复杂性的问题，涉及到多个不同的领域，包括计算机硬件技术、计算机软件技术、网络技术、通信技术以及管理技术等，要解决好网络安全问题，唯有从技术和管理两方面同时着手，才能切实有效地解决问题。

1.4.1　技术角度

要有效地解决网络安全问题，就技术上来讲，必须有一套完整的解决方案才行。下面就网络安全解决方案中的一些基本内容作一些简要说明。

1．网络信息安全系统设计原则

（1）满足分级管理需求；

（2）需求、风险、代价平衡的原则；

（3）综合性、整体性原则；

（4）可用性原则；

（5）分步实施原则。

目前，对于新建网络及已投入运行的网络，必须尽快解决网络的安全保密问题，设计时应遵循如下思想：

（1）提高系统的安全性和保密性；

（2）保持网络原有性能特点，即对网络的协议和传输具有很好的透明性；

（3）易于操作、维护，并便于自动化管理，而不增加或少增加附加操作；

（4）尽量不影响原网络拓扑结构，便于系统及系统功能的扩展；

（5）安全保密系统具有较好的性能价格比，一次性投资，可以长期使用；

（6）安全与密码产品具有合法性，并便于安全管理单位与密码管理单位的检查与监督。

2．网络信息安全系统设计步骤

（1）网络安全需求分析；

（2）确立合理的目标基线和安全策略；

（3）明确准备付出的代价；

（4）制定可行的技术方案；

（5）工程实施方案（产品的选购与定制）；

（6）制定配套的法规、条例和管理办法。

3．网络信息安全解决方案

下面主要从网络安全需求上进行分析，并基于网络层次结构，提出不同层次与安全强度的网络信息安全解决方案。

1）防火墙

防火墙是企业局域网到 Internet 的唯一出口，所有的访问都将通过防火墙进行，防火墙能够有效地保护局域网。防火墙既能保证提供正常的服务，又能有效地保护服务器不受攻击。

2）入侵检测系统

入侵检测系统能够有效地检测各种类型的攻击，通过在网络中不同的位置放置（比如内网、网络引擎），可与中心数据库进行通信，获得安全策略，存储警报信息，并针对入侵启动相应的动作。管理员可在网络中的多个位置访问网络引擎，对入侵检测系统进行监控和管理。

3）网络隐患扫描系统

网络隐患扫描系统能够扫描网络范围内的所有支持 TCP / IP 协议的设备，扫描的对象包括扫描多种操作系统，扫描网络设备包括服务器、工作站、防火墙、路由器和路由交换机等。在进行扫描时，可以从网络中不同的位置对网络设备进行扫描。扫描结束后生成详细的安全评估报告，采用报表和图形的形式对扫描结果进行分析，可以方便直观地对用户进行安全性能评估和检查。

4）网站监测与恢复系统

在 Web 服务器上放置网站实时监控系统服务器，用于监控网页是否被非法改动。网站监控系统的备份服务器和文件上传放置在局域网内部，既能恢复被非法篡改的主页，又能受防火墙的有效保护而不受攻击。同时在公网上也可配置文件上传服务器，用于更新网页内容。

5）网络防病毒

保护整个网络免受病毒侵害，保证网络系统中信息的可用性，构建从主机到服务器的完善的防病毒体系。以服务器作为网络的核心，通过派发的形式对整个网络部署查、杀毒。

6）数据加密及传输安全

通过 VPN 技术，提高各级子网间的信息（如电子公文，MAIL…）传输过程中的保密

性和安全性。

除了上述几个方面以外，再加上计算机安全监控系统和内网安全监控系统，就可以构成一个完整的安全解决方案了，可以大大提高网络信息系统的安全性。

1.4.2　管理角度

从管理角度解决网络安全问题，首先要加强信息安全教育，提高全体人员的安全意识，建立、健全安全操作规范、安全保密制度，积极培养网络安全专门人才，向全体人员提供一定安全技术和技能的培训。总体上讲，可以遵循如下思路。

（1）整体考虑，统一规划。网络安全取决于系统中最薄弱的环节。“一点突破，全网突破”，单个系统考虑安全问题并不能真正有效地保证安全，需要从整体 IT 体系层次建立网络安全架构，整体考虑，全面防护。

（2）战略优先，合理保护。网络安全工作应服从组织信息化建设总体战略，滚动式实现系统安全体系的统一。在此前提之下，追求适度安全，合理保护组织信息资产，安全投入与资产的价值应相匹配。

（3）集中管理，重点防护。统筹设计安全总体架构，建立规范、有序的安全管理流程，集中管理各系统的安全问题，避免安全“孤岛”和安全“短板”。

（4）七分管理，三分技术。管理是企业网络安全的核心，技术是安全管理的保证。只有制定完整的规章制度、行为准则并和安全技术手段合理结合，网络系统的安全才会有最大的保障。

1.5　网络安全的重要性

据《2005 年 FBI 计算机犯罪调查》显示，在过去的 12 个月中，1324 家机构（约占被调查机构总数的 64%）都因计算机安全事故而遭受了财务损失。被调查机构总共损失了 3200 万美元，平均每家机构的成本超过了 24000 美元。

美国联邦调查局（FBI ）称，应对病毒、间谍软件、PC 窃贼，以及其他与计算机相关的犯罪活动每年给美国企业造成了 672 亿美元的负担，FBI 根据对 2066 家机构的调查得出了这一结果。但是，在利用这一调查结果估算全国的损失时，FBI 将受到攻击的企业比例由 64% 下调到了更为保守的 20%，这意味着至少有 280 万家美国企业曾经遭受过一次计算机安全事故，如果按每家企业每年平均 24000 美元的损失计算，这就会给美国企业每年造成 672 亿美元的损失。

PricewaterhouseCoopers 公司在 2005 年 10 月到 2006 年 1 月期间，调查了 1000 家左右的企业，该调查的名称为《DTI 信息安全事故调查》。据 PricewaterhouseCoopers 顾问公司受英国贸易与工业部委托而进行的一项调查的结果显示，预计去年由于计算机病毒、间谍软件、黑客攻击和设备盗窃引发的安全问题令英国企业界在去年损失了 180 亿美元（约合 100 亿英镑），这一水平与两年前相比增长了 50％左右。

尽管各企业花在信息安全控制方面的投资越来越大，现在平均已经达到公司 IT 预算的 4％到 5％，但是与安全问题有关的损失仍然在不断增长。在 2004 年的时候，各企业在信息安全控制方面的投资平均占各自 IT 预算的 3％左右。

根据《中国大陆地区2005年度电脑病毒疫情与网络安全报告》（以下简称《报告》）显示，中国2005年截获的新病毒数量达到72836个，较2004年翻了一番，其中90%以上带有明显商业利益驱动的特征；黑客、病毒和流氓软件的紧密结合已逐渐形成清晰的“产业链条”，而正规的互联网公司正日趋成为黑客和流氓软件的“第一推动力”。

公安机关发布的数据统计显示，2005年，国内处理的网络安全犯罪近3万起，国内网民因为网络安全犯罪而造成的直接损失超过1亿元。银行等国内金融机构成为网络诈骗犯罪高发的“重灾区”，按照GDP和我国网络应用水平计算，国内金融系统全年因网络安全犯罪造成直接经济损失约10亿元人民币。而据综合估测，中国2005年因网络威胁造成的间接损失高达数十亿元。

2004年5月，某大型企业研发中心发现某国外竞争对手领先一步完成了A产品的设计开发，该研发中心领导一下就懵了。A产品的设计开发可是该企业重大研发项目，该企业也想依托A产品完成产品线的转换，企业为该项目投入了大笔资金，众多研发人员也付出了艰辛的劳动。企业在项目立项及开发过程中，还从未听说有哪家单位也在进行A产品的开发，为什么竞争对手开发速度如此之快?

情况汇报给企业老总后，老总第一反应就是内部人员泄密，随即下令该项目所有人员停止开发，迅速离开工作岗位，并向公安部门报案。公安部门技术人员到达现场后发现该研发中心保密工作存在重大疏漏：设计人员电脑与普通工作人员电脑连在同一个局域网内、计算机端口允许人员将资料随意拷出、设计人员将某些机密文件设成共享、打印资料随意带出、所有电脑都可以上互联网……经过检查，公安部门初步判定为内部人员泄密，但是要查出谁将资料泄密，难度太大。最终该案不了了之，企业也只能对研发中心领导进行降职处罚，该企业为此付出了1000余万元研发费用，众多研发人员的辛勤劳动全部付诸东流。

以上仅仅是众多信息安全事件中的一个罢了，所造成的巨大损失主要原因是没有重视网络信息安全，更没有采取有效措施来防范网络信息安全所面临的各种安全威胁。反思该企业的惨痛教训，我们应当引以为戒，切实做好安全保密工作，防范机密资料外泄，同时也应当认识到保密工作也是增加企业价值的重要工作内容。

1.6 网络安全的紧迫性

今年6月，公安部公共信息网络安全监察局对我国2005年5月至2006年5月发生的网络安全事件和安全管理中存在的问题进行了调查，25日发布了2006年全国信息网络安全状况与计算机病毒疫情调查报告。

调查报告显示，在被调查的13,000多家单位中，54%的被调查单位发生过信息网络安全事件，比去年上升5%，其中发生过3次以上的占22%，比去年上升7%。感染计算机病毒、蠕虫和木马程序仍然是最突出的网络安全情况，占发生安全事件总数的84%，“遭到端口扫描或网络攻击”和“垃圾邮件”分别占36%和35%。

在发生的安全事件中，攻击或传播源来自外部的占50%，比去年下降7%；内外部均有的占34.5%，比去年上升10.5%。73%的安全事件是由于未修补或防范软件漏洞所导致。

金融证券行业发生网络安全事件的比例最低，商业贸易、制造业、广电和新闻、教育

科研、互联网和信息技术等行业发生网络安全事件的比例较高。网络用户的安全防范意识在不断增强并切实采取了措施。

从调查报告的内容可以看出，网络安全问题时刻威胁着我们，同时网络安全工作也是一个任重而道远的工作，需要我们不断加强安全意识，积极采取各种安全措施，不断完善和提高网络安全技能和技巧，尽量减少网络安全事件的发生，对已经发生的网络安全事件进行及时处理，将损失降低到最小。

习题

1．简要叙述网络安全所面临的挑战。
2．简述网络安全的内容。
3．简述网络安全问题的解决思路。
4．简述网络安全的重要性和紧迫性。

第 2 章　计算机病毒防范

教学提示

在网络安全的世界中，计算机病毒一直给我们造成了非常大的危害，近的如“冲击波”、“震荡波”病毒，较远的有 CIH、“红色代码”等病毒。计算机病毒的重要特征是发展迅速、种类繁多、破坏性强，所以做好计算机病毒防范工作具有重要的意义。

要做到有效防范计算机病毒，需要对计算机病毒本身以及计算机病毒的防范措施有一个更加深入的了解。本章将对计算机病毒的定义、发展、特点、表现、危害以及防范技术等内容进行讲解，帮助读者建立对计算机病毒的正确认识，通过各种有效的计算机病毒防范措施以达到防止计算机病毒破坏，保护计算机系统安全以及数据安全的目的。

通过对本章的学习，应对计算机病毒的特点、危害、防范意识以及防范技能等方面的认识有所提高，在实际的工作、学习和生活中有效防止计算机病毒的破坏，提高网络系统以及计算机系统的安全性。

教学重点

- 计算机病毒的定义。
- 计算机病毒的特点。
- 计算机病毒的表现。
- 计算机病毒的防范技术。

2.1　计算机病毒的基本概念

计算机病毒是某些人利用计算机软、硬件所固有的脆弱性，编制的具有特殊功能的程序。它能通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活，它用修改其他程序的方法将自己的精确拷贝或者可能演化的形式放入其他程序中，从而感染它们，对计算机资源进行破坏。

2.1.1　什么是计算机病毒

计算机病毒是一个程序，一段可执行码。计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上。当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。

除复制能力外，某些计算机病毒还有其他一些共同特性：一个被感染的程序能够传送病毒载体。当你看到病毒载体似乎仅仅表现在文字和图象上时，它们可能也已毁坏了文件、再格式化你的硬盘驱动或引发了其他类型的灾害。若是病毒并不寄生于一个感染程序，它仍然能通过占据存储空间带来麻烦，并降低计算机的全部性能。

可以从不同角度给出计算机病毒的定义。

（1）计算机病毒是通过磁盘、磁带和网络等媒介传播扩散，能“传染” 其他程序的程序。

（2）计算机病毒是能够实现自身复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序。

（3）计算机病毒是一种人为制造的程序，它通过不同的途径潜伏或寄生在存储媒体（如磁盘、内存）或程序里，当某种条件或时机成熟时，它会自生复制并传播，使计算机的资源受到不同程度的破坏等等。

这些说法在某种程度上说明了计算机病毒的某些特征，只是不够全面和具体。1994 年 2 月 18 日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》，在《条例》第二十八条中明确对计算机病毒下了定义：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。”此定义具有规范性、权威性。

2.1.2　计算机病毒的命名

当杀毒软件发现计算机上有病毒时，通常会给出一个提示窗口，窗口中给出了所发现病毒的相关信息。杀毒软件诺顿发现病毒时的提示窗口类似图 2-1 所示。可以看到，病毒名称为 Backdoor.Formador，要了解这个名称所代表的意思，就需要了解计算机病毒的命名规则。

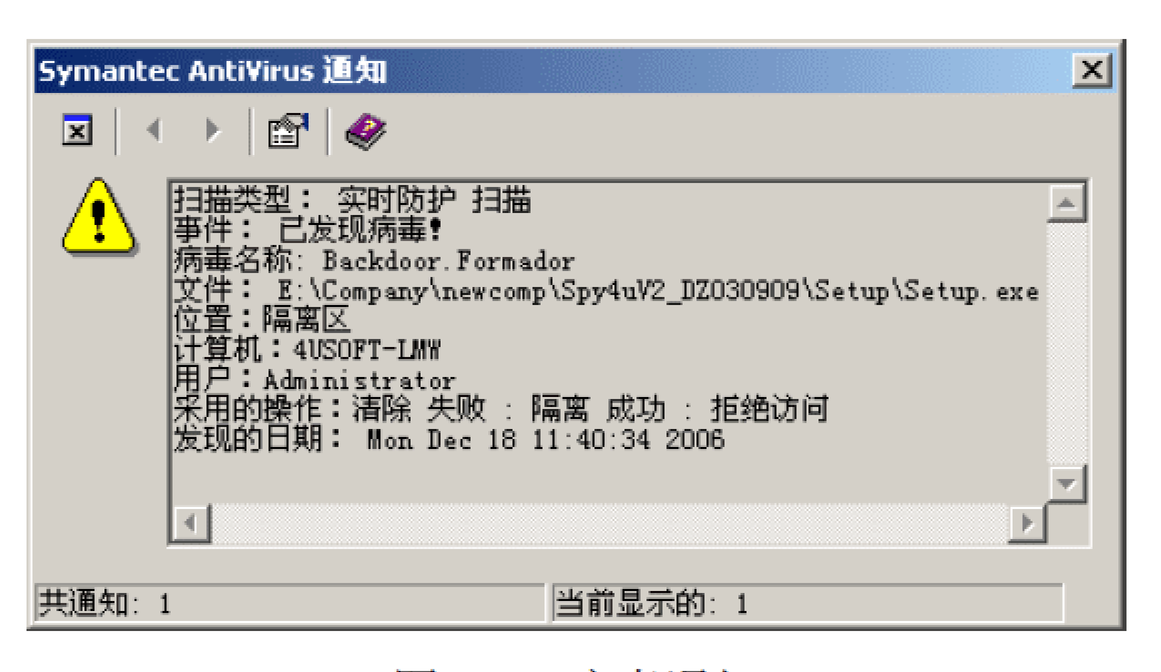


图 2-1　病毒通知

计算机病毒很多，而且发展迅速，所以反病毒公司为了方便管理，他们按照病毒的特性，将病毒进行分类命名。虽然各个反病毒公司的命名规则都不太一样，但大体都是采用一个统一的命名方法来命名的。

一般格式：<病毒前缀>.<病毒名>.<病毒后缀> 。

病毒前缀是指一个病毒的种类，是用来区别病毒的种族分类的。不同种类的病毒，其前缀也是不同的。比如常见的木马病毒的前缀是 Trojan，蠕虫病毒的前缀是 Worm。

病毒名是指一个病毒的家族特征，是用来区别和标识病毒家族的，如以前著名的 CIH 病毒的家族名都是统一的 CIH，振荡波蠕虫病毒的家族名是 Sasser。

病毒后缀是指一个病毒的变种特征，是用来区别具体某个家族病毒的某个变种的。一般都采用英文中的 26 个字母来表示，如 Worm.Sasser.b 就是指振荡波蠕虫病毒的变种 B，因此一般称为“振荡波 B 变种”或者“振荡波变种 B”。如果该病毒变种非常多，可以采用数字与字母混合表示变种标识。

综上所述，一个病毒的前缀对我们快速的判断该病毒属于哪种类型的病毒是有非常大

的帮助。通过判断病毒的类型，就可以对这个病毒有个大概的评估。而通过病毒名我们可以利用查找资料等方式进一步了解该病毒的详细特征。病毒后缀能让我们知道现在你的计算机所感染的病毒是哪个变种，有利于寻找对应的解决方法。

2.1.3 计算机病毒的分类

下面对常见的计算机病毒种类进行说明。

1．系统病毒

系统病毒的前缀为 Win32、PE、Win95、W32、W95 等。这些病毒的一般公有的特性是可以感染 Windows 操作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播。如 CIH 病毒。

2．蠕虫病毒

蠕虫病毒的前缀是 Worm。这种病毒的公有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带病毒邮件，阻塞网络的特性。比如冲击波（阻塞网络），小邮差（发带病毒邮件）等。

3．木马病毒、黑客病毒

木马病毒其前缀是 Trojan，黑客病毒前缀名一般为 Hack。木马病毒的公有特性是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息，而黑客病毒则有一个可视的界面，能对用户的计算机进行远程控制。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的计算机，而黑客病毒则会通过该木马病毒来进行控制。

现在这两种类型都越来越趋向于整合了。一般的木马如 QQ 消息尾巴木马 Trojan.QQ3344，还有大家可能遇见比较多的针对网络游戏的木马病毒如 Trojan.LMir.PSW.60。黑客程序如网络枭雄 Hack.Nether.Client。

> **提示：**病毒名中有 PSW 或者什么 PWD 之类的一般都表示这个病毒有盗取密码的功能，这些字母一般都为“密码”的英文“password”的缩写。

4．脚本病毒

脚本病毒的前缀是 Script。脚本病毒的公有特性是使用脚本语言编写，通过网页进行传播的病毒，如红色代码（Script.Redlof）。脚本病毒还会有前缀：VBS、JS（表明是何种脚本编写的，其中 VBS 表示 VBScript 脚步语言编写，JS 表示 JavaScript 脚本语言编写），如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

5．宏病毒

其实宏病毒也是脚本病毒的一种，由于它的特殊性，因此在这里单独算成一类。宏病毒的前缀是 Macro，第二前缀是 Word、Word97、Excel、Excel97 等。

（1）只感染 Word97 及以前版本 Word 文档的病毒采用 Word97 作为第二前缀，格式是 Macro.Word97。

（2）只感染 Word97 以后版本 Word 文档的病毒采用 Word 作为第二前缀，格式是 Macro.Word。

（3）只感染 Excel97 及以前版本 Excel 文档的病毒采用 Excel97 作为第二前缀，格式是 Macro.Excel97。

（4）凡是只感染 Excel97 以后版本 Excel 文档的病毒采用 Excel 作为第二前缀，格式是 Macro.Excel。

依此类推。

该类病毒的公有特性是能感染 Office 系列文档，然后通过 Office 模板进行传播，如著名的美丽莎（Macro.Melissa）。

6．后门病毒

后门病毒的前缀是 Backdoor。该类病毒的公有特性是通过网络传播，给系统开后门，给用户计算机带来安全隐患。如很多朋友遇到过的 IRC 后门 Backdoor.IRCBot 。

7．病毒种植程序病毒

这类病毒的公有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏。如：冰河播种者（Dropper.BingHe2.2C）、MSN 射手（Dropper.Worm.Smibag）等。

8．破坏性程序病毒

破坏性程序病毒的前缀是 Harm。这类病毒的公有特性是本身具有好看的图标来诱惑用户单击，当用户单击这类病毒时，病毒便会直接对用户计算机产生破坏。如：格式化 C 盘（Harm.formatC.f）、杀手命令（Harm.Command.Killer）等。

9．玩笑病毒

玩笑病毒的前缀是 Joke，也称恶作剧病毒。这类病毒的公有特性是本身具有好看的图标来诱惑用户单击，当用户单击这类病毒时，病毒会做出各种破坏操作来吓唬用户，其实病毒并没有对用户计算机进行任何破坏。如女鬼（Joke.Girlghost）病毒。

10．捆绑机病毒

捆绑机病毒的前缀是 Binder。这类病毒的公有特性是病毒作者会使用特定的捆绑程序将病毒与一些应用程序如 QQ、IE 捆绑起来，表面上看是一个正常的文件，当用户运行这些文件时，会表面上运行这些应用程序，然后隐藏运行捆绑在一起的病毒，从而给用户造成危害，如捆绑 QQ（Binder.QQPass.QQBin）、系统杀手（Binder.killsys）等。

除了上述的类型以外还有其他的，不过比较少见，所以在此不一一列举。通过上面的介绍，可以在查出某个病毒以后通过以上所说的方法来初步判断所中病毒的基本情况，尤其是在杀毒软件无法杀掉病毒的情况下，通过病毒名称更容易查找相关资料。

2.2　计算机病毒的特点及表现现象

从实质上说，计算机病毒是一段程序代码，虽然它可能隐藏得很好，但也会留下许多痕迹。通过对这些蛛丝马迹的判别，就能发现计算机病毒的存在。

根据计算机病毒感染和发作的阶段，可以将计算机病毒的表现现象分为三大类，即计算机病毒发作前、发作时和发作后的表现现象。介绍计算机病毒的表现现象之前，先介绍一下计算机病毒的特点。

2.2.1 计算机病毒的特点

计算机病毒一般具有以下特性。

1. 计算机病毒的可执行性

计算机病毒与其他合法程序一样，是一段可执行的程序，但它不是一个完整的程序，而是寄生在其他可执行的程序上，因此它享有一切程序所能得到的权力。在病毒运行时，与合法程序争夺系统的控制权。计算机病毒只有当它在计算机内得以运行时，才具有传染性和破坏性等活性。也就是说计算机 CPU 的控制权是关键问题。 若计算机在正常程序控制下运行，而不运行带病毒的程序，则这台计算机总是可靠的。在这台计算机上可以查看病毒文件的名字，查看计算机病毒的代码，打印病毒的代码，甚至复制病毒程序，却都不会感染上病毒。反病毒技术人员整天就是在这样的环境下工作。他们的计算机虽也存有各种计算机病毒的代码，但已置这些病毒于控制之下，计算机不会运行病毒程序，整个系统是安全的。相反，计算机病毒一经在计算机上运行，在同一台计算机内病毒程序与正常系统程序，或某种病毒与其他病毒程序争夺系统控制权时往往会造成系统崩溃，导致计算机瘫痪。反病毒技术就是要提前取得计算机系统的控制权，识别出计算机病毒的代码和行为，阻止其取得系统控制权。反病毒技术的优劣就是体现在这一点上。一个好的抗病毒系统应该不仅能可靠地识别出已知计算机病毒的代码，阻止其运行或旁路掉其对系统的控制权（实现安全带毒运行被感染程序），还应该识别出未知计算机病毒在系统内的行为，阻止其传染和破坏系统的行动。

2. 计算机病毒的传染性

传染性是病毒的基本特征。在生物界，病毒通过传染从一个生物体扩散到另一个生物体。在适当的条件下，它可以得到大量繁殖，并使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么病毒会在这台机子上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染源，再与其他机器进行数据交换或通过网络接触，病毒会继续进行传染。

正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的。而病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。计算机病毒可通过各种可能的渠道，如软盘、计算机网络去传染其他的计算机。当您在一台机器上发现了病毒时，往往曾在这台计算机上用过的软盘已感染上了病毒，而与这台机器相联网的其他计算机也许也被该病毒染上了。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。

病毒程序通过修改磁盘扇区信息或文件内容并把自身嵌入到其中的方法达到病毒的传染和扩散。被嵌入的程序叫做宿主程序。

3. 计算机病毒的潜伏性

一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，可以在几周或者

几个月内甚至几年内隐藏在合法文件中，对其他系统进行传染，而不被人发现，潜伏性愈好，其在系统中的存在时间就会愈长，病毒的传染范围就会愈大。

潜伏性的第一种表现是指，病毒程序不用专用检测程序是检查不出来的，因此病毒可以静静地躲在磁盘或磁带里待上几天，甚至几年，一旦时机成熟，得到运行机会，就又要四处繁殖、扩散，继续为害。潜伏性的第二种表现是指，计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染外不做什么破坏工作。触发条件一旦得到满足，有的在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、对数据文件做加密、封锁键盘以及使系统死锁等。

4．计算机病毒的可触发性

病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己，病毒必须潜伏，少做动作。如果完全不动，一直潜伏的话，病毒既不能感染也不能进行破坏，便失去了杀伤力。病毒既要隐蔽又要维持杀伤力，它必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，病毒继续潜伏。

5．计算机病毒的破坏性

所有的计算机病毒都是一种可执行程序，而这一可执行程序又必然要运行，所以对系统来讲，所有的计算机病毒都存在一个共同的危害，即降低计算机系统的工作效率，占用系统资源，其具体情况取决于入侵系统的病毒程序。

计算机病毒的破坏性主要取决于计算机病毒设计者的目的。如果病毒设计者的目的在于彻底破坏系统的正常运行的话，那么这种病毒对于计算机系统进行攻击造成的后果是难以设想的，它可以毁掉系统的部分数据，也可以破坏全部数据并使之无法恢复。但并非所有的病毒都对系统产生极其恶劣的破坏作用。有时几种本没有多大破坏作用的病毒交叉感染，也会导致系统崩溃等重大恶果。

6．攻击的主动性

病毒对系统的攻击是主动的，不以人的意志为转移的。也就是说，从一定的程度上讲，计算机系统无论采取多么严密的保护措施都不可能彻底地排除病毒对系统的攻击，而保护措施充其量是一种预防的手段而已。

7．病毒的针对性

计算机病毒是针对特定的计算机和特定的操作系统的。例如，有针对 1BM　PC 及其兼容机的，有针对 App1e 公司的 Macintosh 的，还有针对 UNIX 操作系统的。例如小球病毒是针对 IBM　PC 及其兼容机上的 DOS 操作系统的。

8．病毒的非授权性

病毒未经授权而执行。一般正常的程序是由用户调用，再由系统分配资源，完成用户交给的任务。其目的对用户是可见的、透明的。而病毒具有正常程序的一切特性，它隐藏在正常程序中，当用户调用正常程序时窃取到系统的控制权，先于正常程序执行，病毒的动作、目的对用户来说是未知的，是未经用户允许的。

9．病毒的隐蔽性

病毒一般是具有很高编程技巧，短小精悍的程序。通常附在正常程序中或磁盘较隐蔽的地方，也有个别的以隐含文件形式出现。目的是不让用户发现它的存在。如果不经过代码分析，病毒程序与正常程序是不容易区别开来的。一般在没有防护措施的情况下，计算机病毒程序取得系统控制权后，可以在很短的时间里传染大量程序。而且受到传染后，计算机系统通常仍能正常运行，使用户不会感到任何异常，好像不曾在计算机内发生过什么。试想，如果病毒在传染到计算机上之后，机器马上无法正常运行，那么它本身便无法继续进行传染了。正是由于隐蔽性，计算机病毒得以在用户没有察觉的情况下扩散并游荡于世界上百万台计算机中。

大部分的病毒的代码之所以设计得非常短小，也是为了隐藏。病毒一般只有几百或 1K 字节，而 PC 对 DOS 文件的存取速度可达每秒几百 KB 以上，所以病毒转瞬之间便可将这短短的几百个字节附着到正常程序之中，使人非常不易察觉。

计算机病毒的隐蔽性表现在两个方面。

（1）传染的隐蔽性。大多数病毒在进行传染时速度是极快的，一般不具有外部表现，不易被人发现。我们设想，如果计算机病毒每当感染一个新的程序时都在屏幕上显示一条信息“我是病毒程序，我要干坏事了”，那么计算机病毒早就被控制住了。确实有些病毒非常“勇于暴露自己”，时不时在屏幕上显示一些图案或信息，或演奏一段乐曲。往往此时那台计算机内已有许多病毒的拷贝了。许多计算机用户对计算机病毒没有任何概念，更不用说心理上的警惕了。他们见到这些新奇的屏幕显示和音响效果，还以为是来自计算机系统，而没有意识到这些病毒正在损害计算机系统，正在制造灾难。

（2）病毒程序存在的隐蔽性。一般的病毒程序都夹在正常程序之中，很难被发现，而一旦病毒发作出来，往往已经给计算机系统造成了不同程度的破坏。被病毒感染的计算机在多数情况下仍能维持其部分功能，不会由于一感染上病毒，整台计算机就不能启动了，或者某个程序一旦被病毒所感染，就被损坏得不能运行了。如果出现这种情况，病毒也就不能传播得那么快了。计算机病毒设计的精巧之处也在这里。正常程序被计算机病毒感染后，其原有功能基本上不受影响，病毒代码附于其上而得以存活，得以不断地得到运行的机会，去传染出更多的复制体，与正常程序争夺系统的控制权和磁盘空间，不断地破坏系统，导致整个系统的瘫痪。病毒的代码设计得非常精巧而又短小。

10．病毒的衍生性

这种特性为一些好事者提供了一种创造新病毒的捷径。

分析计算机病毒的结构可知，传染的破坏部分反映了设计者的设计思想和设计目的。但是，这可以被其他掌握原理的人以其个人的企图进行任意改动，从而又衍生出一种不同于原版本的新的计算机病毒（又称为变种）。这就是计算机病毒的衍生性。这种变种病毒造成的后果可能比原版病毒严重得多。

11．病毒的依附性

病毒程序嵌入到宿主程序中，依赖于宿主程序的执行而生存，这就是计算机病毒的寄生性。病毒程序在侵入到宿主程序中后，一般对宿主程序进行一定的修改，宿主程序一旦执行，病毒程序就被激活，从而可以进行自我复制和繁衍。

12．病毒的不可预见性

从对病毒的检测方面来看，病毒还有不可预见性。不同种类的病毒，它们的代码千差万别，但有些操作是共有的（如驻内存，改中断）。有些人利用病毒的这种共性，制作了声称可查所有病毒的程序。这种程序的确可查出一些新病毒，但由于目前的软件种类极其丰富，且某些正常程序也使用了类似病毒的操作甚至借鉴了某些病毒的技术。使用这种方法对病毒进行检测势必会造成较多的误报情况。而且病毒的制作技术也在不断地提高，病毒对反病毒软件永远是超前的。新一代计算机病毒甚至连一些基本的特征都隐藏了，有时可通过观察文件长度的变化来判别。然而，更新的病毒也可以在这个问题上蒙蔽用户，它们利用文件中的空隙来存放自身代码，使文件长度不变。许多新病毒则采用变形来逃避检查，这也成为新一代计算机病毒的基本特征。

13．计算机病毒的欺骗性

计算机病毒行动诡秘，计算机对其反应迟钝，往往把病毒造成的错误当成事实接受下来，故它很容易获得成功。

14．计算机病毒的持久性

即使在病毒程序被发现以后，数据和程序以至操作系统的恢复都非常困难。特别是在网络操作情况下，由于病毒程序由一个受感染的拷贝通过网络系统反复传播，使得病毒程序的清除非常复杂。

2.2.2　计算机病毒发作前的表现现象

计算机病毒发作前，是指从计算机病毒感染计算机系统，潜伏在系统内开始，一直到激发条件满足，计算机病毒发作之前的一个阶段。在这个阶段，计算机病毒的行为主要是以潜伏、传播为主。计算机病毒会以各式各样的手法来隐藏自己，在不被发现同时，又自我复制，以各种手段进行传播。

以下是一些计算机病毒发作前常见的表现现象。

1．平时运行正常的计算机突然经常性无缘无故地死机

病毒感染了计算机系统后，将自身驻留在系统内并修改了中断处理程序等，引起系统工作不稳定，造成死机现象发生。

2．操作系统无法正常启动

关机后再启动，操作系统报告缺少必要的启动文件，或启动文件被破坏，系统无法启动。这很可能是计算机病毒感染系统文件后使得文件结构发生变化，无法被操作系统加载、引导。

3．运行速度明显变慢

在硬件设备没有损坏或更换的情况下，本来运行速度很快的计算机，运行同样应用程序，速度明显变慢，而且重启后依然很慢。这很可能是计算机病毒占用了大量的系统资源，并且自身的运行占用了大量的处理器时间，造成系统资源不足，运行变慢。

4．以前能正常运行的软件经常发生内存不足的错误

某个以前能够正常运行的程序，程序启动的时候报系统内存不足，或者使用应用程序中的某个功能时报说内存不足。这可能是计算机病毒驻留后占用了系统中大量的内存空间，使得可用内存空间减小。需要注意的是在 Windows 95/98 下，记事本程序所能够编辑的文

本文件不超过 64KB，如果用“复制 / 粘贴”操作粘贴一段很大的文字到记事本程序时，也会报“内存不足，不能完成操作”的错误，但这不是计算机病毒在作怪。

5．打印和通信发生异常

硬件没有更改或损坏的情况下，以前工作正常的打印机，近期发现无法进行打印操作，或打印出来的是乱码。串口设备无法正常工作，比如调制解调器不拨号。这很可能是计算机病毒驻留内存后占用了打印端口、串行通信端口的中断服务程序，使之不能正常工作。

6．无意中要求对软盘进行写操作

没有进行任何读、写软盘的操作，操作系统提示软驱中没有插入软盘，或者要求在读取、复制写保护的软盘上的文件时打开软盘的写保护。这很可能是计算机病毒自动查找软盘是否在软驱中的时候引起的系统异常。需要注意的是有些编辑软件需要在打开文件的时候创建一个临时文件，也有的安装程序（如 Office 97）对软盘有写的操作。

7．以前能正常运行的应用程序经常发生死机或者非法错误

在硬件和操作系统没有进行改动的情况下，以前能够正常运行的应用程序产生非法错误和死机的情况明显增加。这可能是由于计算机病毒感染应用程序后破坏了应用程序本身的正常功能，或者计算机病毒程序本身存在着兼容性方面的问题造成的。

8．系统文件的时间、日期、大小发生变化

这是最明显的计算机病毒感染迹象。计算机病毒感染应用程序文件后，会将自身隐藏在原始文件的后面，文件大小大多数会有所增加，文件的访问、修改日期和时间也会被改成感染时的时间。尤其是对那些系统文件，绝大多数情况下是不会修改它们的，除非是进行系统升级或打补丁。对应用程序使用到的数据文件、文件大小和修改日期、时间是可能会改变的，并不一定是计算机病毒在作怪。

9．Word 文件另存时只能以模板方式保存

无法“另存为”一个 DOC 文档，只能保存成模板文档（DOT）。这往往是打开的 Word 文档中感染了 Word 宏病毒的缘故。

10．磁盘空间迅速减少

没有安装新的应用程序，而系统可用的磁盘空间减少得很快。这可能是计算机病毒感染造成的。需要注意的是经常浏览网页、回收站中的文件过多、临时文件夹下的文件数量过多过大、计算机系统有过意外断电等情况也可能会造成可用的磁盘空间迅速减少。另一种情况是 Windows 95/98 下的内存交换文件的增长，在 Windows 95/98 下内存交换文件会随着应用程序运行的时间和进程的数量增加而增长，一般不会减少，而且同时运行的应用程序数量越多，内存交换文件就越大。

11．网络驱动器卷或共享目录无法调用

对于有读权限的网络驱动器卷、共享目录等无法打开、浏览，或者对有写权限的网络驱动器卷、共享目录等无法创建、修改文件。虽然目前还很少有纯粹地针对网络驱动器卷和共享目录的计算机病毒，但计算机病毒的某些行为可能会影响对网络驱动器卷和共享目录的正常访问。

12．基本内存发生变化

在 DOS 下用 mem /c/p 命令查看系统中内存使用状况的时候可以发现基本内存总字节数比正常的 640KB 要小，一般少 1～2KB。这通常是计算机系统感染了引导型计算机病毒

所造成的。

13．陌生人发来的电子函件

收到陌生人发来的电子函件，尤其是那些标题很具诱惑力，比如一则笑话，或者一封情书等，又带有附件的电子函件。当然，这要与广告电子函件、垃圾电子函件和电子函件炸弹区分开。一般来说广告电子函件有很明确的推销目的，会有它推销的产品介绍；垃圾电子函件的内容要么自成章回，要么根本没有价值。这两种电子函件大多是不会携带附件的。电子函件炸弹虽然也带有附件，但附件一般都很大，少则上兆字节，多的有几十兆甚至上百兆字节，而电子函件计算机病毒的附件大多是脚本程序，通常不会超过 100KB。当然，电子函件炸弹在一定意义上也可以看成是一种黑客程序，是一种计算机病毒。

14．自动连接到一些陌生的网站

没有在上网，计算机会自动拨号并连接到因特网上一个陌生的站点，或者在上网的时候发现网络特别慢，存在陌生的网络连接。这种连接大多是黑客程序将收集到的计算机系统的信息“悄悄地”发回某个特定的网址，可以通过 netstat 命令查看当前建立的网络连接，再比照访问的网站来发现。需要注意的是有些网页中有一些脚本程序会自动连接到一些网页评比站点，或者是广告站点，这时候也会有陌生的网络连接出现。当然，这种情况也可以认为是非法的。

一般的系统故障是有别于计算机病毒感染的。系统故障大多只符合上面的一点或二点现象，而计算机病毒感染所出现的现象会多得多。根据上述几点，就可以初步判断计算机和网络是否感染上了计算机病毒。

2.2.3　计算机病毒发作时的表现现象

计算机病毒发作时是指满足计算机病毒发作的条件，计算机病毒程序开始破坏行为的阶段。计算机病毒发作时的表现大都各不相同，可以说一百个计算机病毒发作有一百种花样。这与编写计算机病毒者的心态、所采用的技术手段等都有密切的关系。

以下列举了一些计算机病毒发作时常见的表现现象。

1．提示一些不相干的话

最常见的是提示一些不相干的话，比如打开感染了宏病毒的 Word 文档，如果满足了发作条件的话，它就会弹出对话框显示“这个世界太黑暗了！”，并且要求输入“太正确了”后按确定按钮。

2．发出一段的音乐

恶作剧式的计算机病毒，最著名的是外国的“杨基”计算机病毒（Yangkee）和中国的“浏阳河”计算机病毒。“杨基”计算机病毒发作是利用计算机内置的扬声器演奏《杨基》音乐，而“浏阳河”计算机病毒更绝，当系统时钟为 9 月 9 日时演奏歌曲《浏阳河》，而当系统时钟为 12 月 26 日时则演奏《东方红》的旋律。这类计算机病毒大多属于“良性”计算机病毒，只是在发作时发出音乐和占用处理器资源。

3．产生特定的图象

另一类恶作剧式的计算机病毒，比如小球计算机病毒，发作时会从屏幕上方不断掉落下来小球图形。单纯地产生图像的计算机病毒大多也是“良性”计算机病毒，只是在发作时破坏用户的显示界面，干扰用户的正常工作。

4. 硬盘灯不断闪烁

硬盘灯闪烁说明有硬盘读写操作。当对硬盘有持续大量的操作时，硬盘的灯就会不断地闪烁，比如格式化或者写入很大的文件。有时候对某个硬盘扇区或文件反复读取的情况下也会造成硬盘灯不断闪烁。有的计算机病毒会在发作的时候对硬盘进行格式化，或者写入许多垃圾文件，或反复读取某个文件，致使硬盘上的数据遭到损失。具有这类发作现象的计算机病毒大多是“恶性”计算机病毒。

5. 进行游戏算法

有些恶作剧式的计算机病毒发作时采取某些算法简单的游戏来中断用户的工作，一定要玩赢了才让用户继续他的工作。比如曾经流行一时的“台湾一号”宏病毒，在系统日期为 13 日时发作，弹出对话框，要求用户做算术题。这类计算机病毒一般是属于“良性”计算机病毒，但也有那种用户输了后进行破坏的“恶性”计算机病毒。

6. Windows 桌面图标发生变化

这一般也是恶作剧式的计算机病毒发作时的表现现象。把 Windows 默认的图标改成其他样式的图标，或者将其他应用程序、快捷方式的图标改成 Windows 默认图标样式，起到迷惑用户的作用。

7. 计算机突然死机或重启

有些计算机病毒程序兼容性上存在问题，代码没有严格测试，在发作时会造成意想不到情况；或者是计算机病毒在 Autoexec.bat 文件中添加了一句 Format c：之类的语句，需要系统重启后才能实施破坏的。

8. 自动发送电子函件

大多数电子函件计算机病毒都采用自动发送电子函件的方法作为传播的手段，也有的电子函件计算机病毒在某一特定时刻向同一个邮件服务器发送大量无用的信件，以达到阻塞该邮件服务器的正常服务功能。

9. 鼠标自己在动

没有对计算机进行任何操作，也没有运行任何演示程序、屏幕保护程序等，而屏幕上的鼠标自己在动，应用程序自己在运行，有受遥控的现象。大多数情况下是计算机系统受到了黑客程序的控制，从广义上说这也是计算机病毒发作的一种现象。

需要指出的是，有些是计算机病毒发作的明显现象，比如提示一些不相干的话、播放音乐或者显示特定的图像等。有些现象则很难直接判定是计算机病毒的表现现象，比如硬盘灯不断闪烁，当同时运行多个内存占用大的应用程序，比如 3ds Max，Adobe Premiere 等，而计算机本身性能又相对较弱的情况下，在启动和切换应用程序的时候也会使硬盘不停地工作，硬盘灯不断闪烁。

2.2.4 计算机病毒发作后的表现现象

通常情况下，计算机病毒发作都会给计算机系统带来破坏性的后果，那种只是恶作剧式的“良性”计算机病毒只是计算机病毒家族中的很小一部分。大多数计算机病毒都是属于“恶性”计算机病毒。“恶性”计算机病毒发作后往往会带来很大的损失，以下列举一些恶性计算机病毒发作后所造成的后果。

1．硬盘无法启动，数据丢失

计算机病毒破坏了硬盘的引导扇区后，就无法从硬盘启动计算机系统了。有些计算机病毒修改了硬盘的关键内容（如文件分配表，根目录区等），使得原先保存在硬盘上的数据几乎完全丢失。

2．系统文件丢失或被破坏

通常系统文件是不会被删除或修改的，除非对计算机操作系统进行了升级。但是某些计算机病毒发作时删除了系统文件，或者破坏了系统文件，使得以后无法正常启动计算机系统。通常容易受攻击的系统文件有 Command.com，Emm386.exe，Win.com，Kernel.exe，User.exe 等等。

3．文件目录发生混乱

目录发生混乱有两种情况。一种情况就是确实将目录结构破坏，将目录扇区作为普通扇区，填写一些无意义的数据，再也无法恢复。另一种情况就是将真正的目录区转移到硬盘的其他扇区中，只要内存中存有该计算机病毒，它就能够将正确的目录扇区读出，并在应用程序需要访问该目录的时候提供正确的目录项，使得从表面上看来与正常情况没有两样。但是一旦内存中没有该计算机病毒，那么通常的目录访问方式将无法访问到原先的目录扇区。这种破坏还是能够被恢复的。

4．部分文档丢失或被破坏

类似系统文件的丢失或被破坏，有些计算机病毒在发作时会删除或破坏硬盘上的文档，造成数据丢失。

5．部分文档自动加密码

还有些计算机病毒利用加密算法，将加密密钥保存在计算机病毒程序体内或其他隐蔽的地方，而被感染的文件被加密，如果内存中驻留有这种计算机病毒，那么在系统访问被感染的文件时它自动将文档解密，使得用户察觉不到。一旦这种计算机病毒被清除，那么被加密的文档就很难被恢复了。

6．修改 Autoexec.bat 文件，增加 Format C：命令

在计算机系统稳定工作后，一般很少会有用户去注意 Autoexec.bat 文件的变化，但是这个文件在每次系统重新启动的时候都会被自动运行，计算机病毒修改这个文件从而达到破坏系统的目的。

7．可使部分软件升级主板的 BIOS 程序混乱，主板被破坏

类似 CIH 计算机病毒发作后的现象，系统主板上的 BIOS 被计算机病毒改写、破坏，使得系统主板无法正常工作，从而使计算机系统报废。

8．网络瘫痪，无法提供正常的服务

由上所述，我们可以了解到防杀计算机病毒软件必须要实时化，在计算机病毒进入系统时要立即报警并清除，这样才能确保系统安全，待计算机病毒发作后再去杀毒，实际上已经为时已晚。

2.3　计算机病毒检测方法

计算机感染病毒以后通常会表现出一些异常的情况，特别明显的几种情况包括计算机

运行速度变慢、上网的速度变慢、出现非法操作提示等，此时就需要通过工具来检测计算机中感染病毒的情况。

2.3.1 手动检测病毒的常用辅助工具

计算机病毒的种类非常多，对计算机用户造成的影响也是各种各样，有部分病毒程序只会造成使用上的不方便，并不会对系统造成灾难性的破坏，此时我们可以借助一些辅助工具来进行检测，常用的辅助工具包括以下几种。

1．进程查看工具

通过进程查看工具可以了解系统中当前运行进程的各种信息，有利于及时发现非法运行的进程以及合法进程中出现的异常现象，在此推荐的工具为 Process Explorer，下面对该工具的基本用法做一个简单的说明。

提示：Process Explorer 工具可以从网站下载，下载网站为 http://www.sysinternals.com。

（1）找到工具程序，启动该程序以后，其主界面如图 2-2 所示。

（2）双击进程列表中的任何一个进程，出现进程相关信息窗口，比如，双击 iexplore.exe 进程，出现如图 2-3 所示。

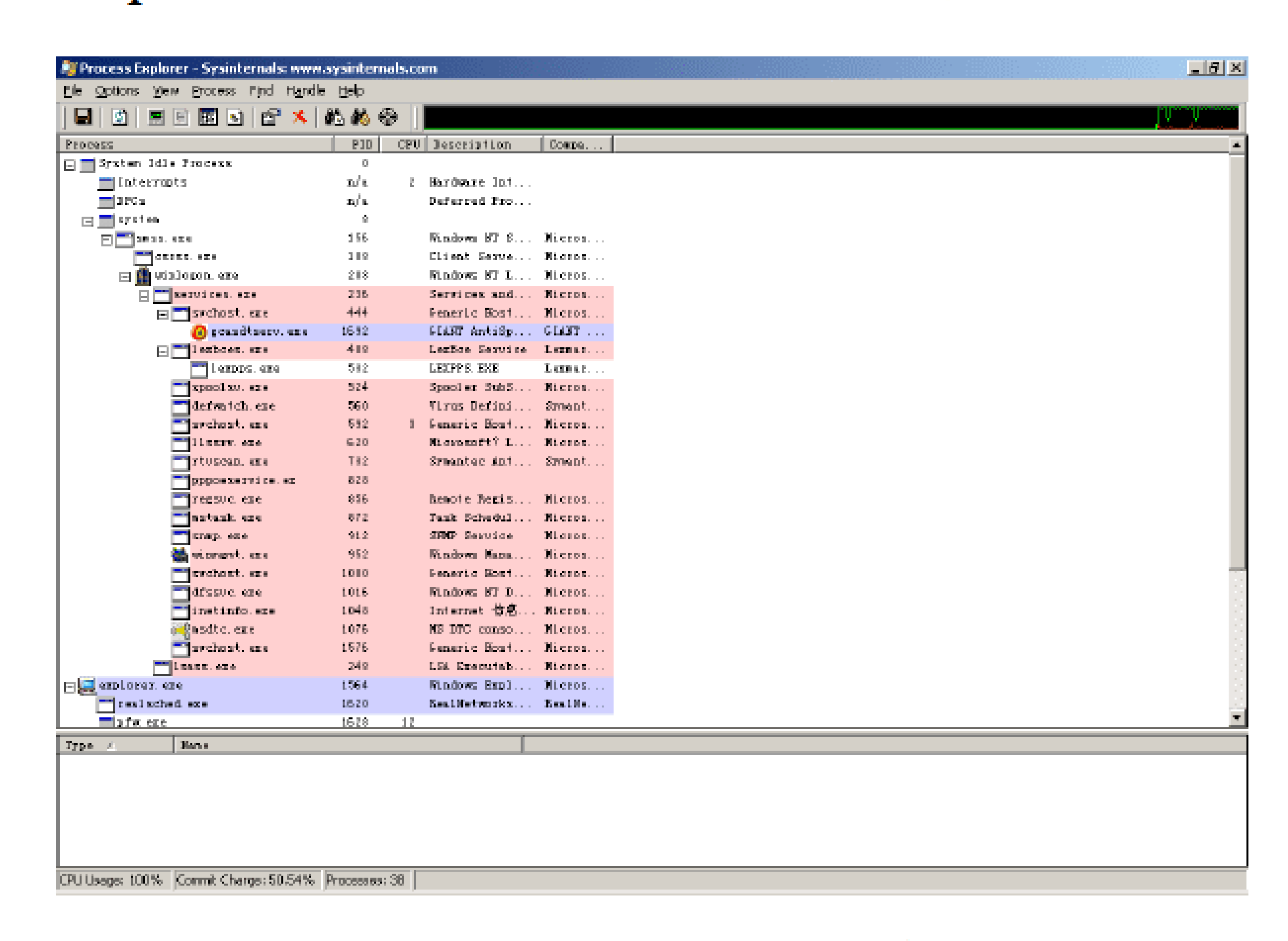


图 2-2 Process Explorer 主窗口

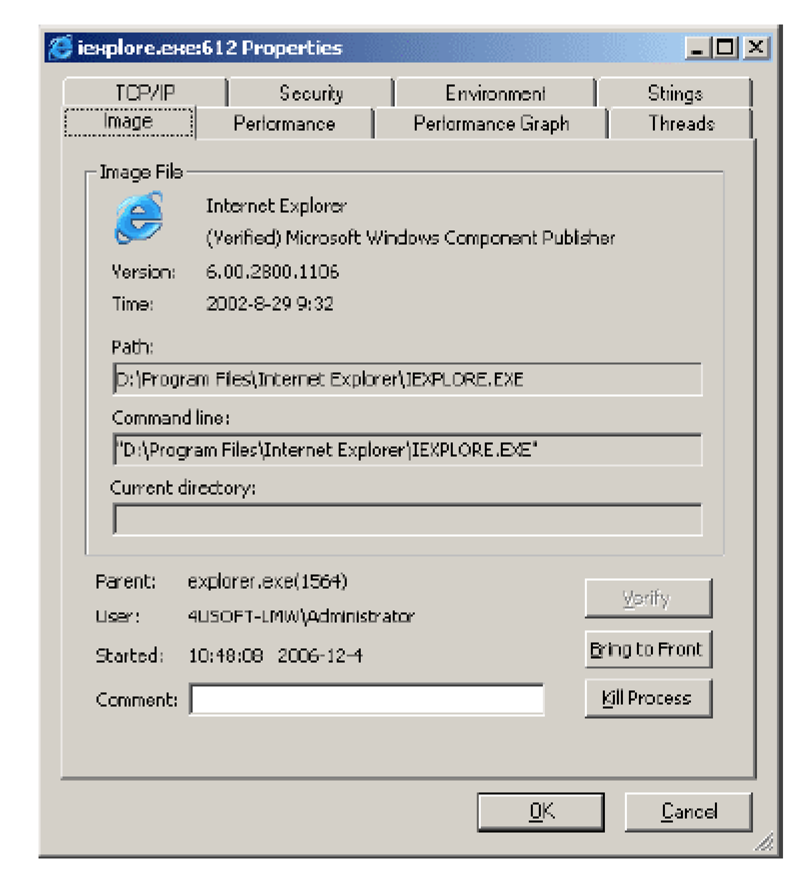


图 2-3 进程信息窗口

（3）在进程信息窗口中，包含大量与进程相关的信息，这些信息通过窗口上的选项卡进行分别显示。单击对应的选项卡就可以看到对应的信息，比如单击 Threads 选项卡就可以进程当前的线程信息，如图 2-4 所示。

（4）在线程信息显示窗口中，如果发现非法线程，可以通过单击 Kill 按钮来结束该线程，此时会出现提示框，提示用户是否确实要结束线程，因为如果强行结束某些重要线程，会导致进程甚至系统崩溃。通过单击 Module 按钮，可以查看线程对应的文件，如图 2-5 所示。

（5）通过对线程对应的文件信息通常可以看出是否是系统中的正常线程还是非法线程，除此之外，在线程信息窗口上还可以单击 Stack 按钮，获得线程的堆栈信息，如图 2-6 所示。

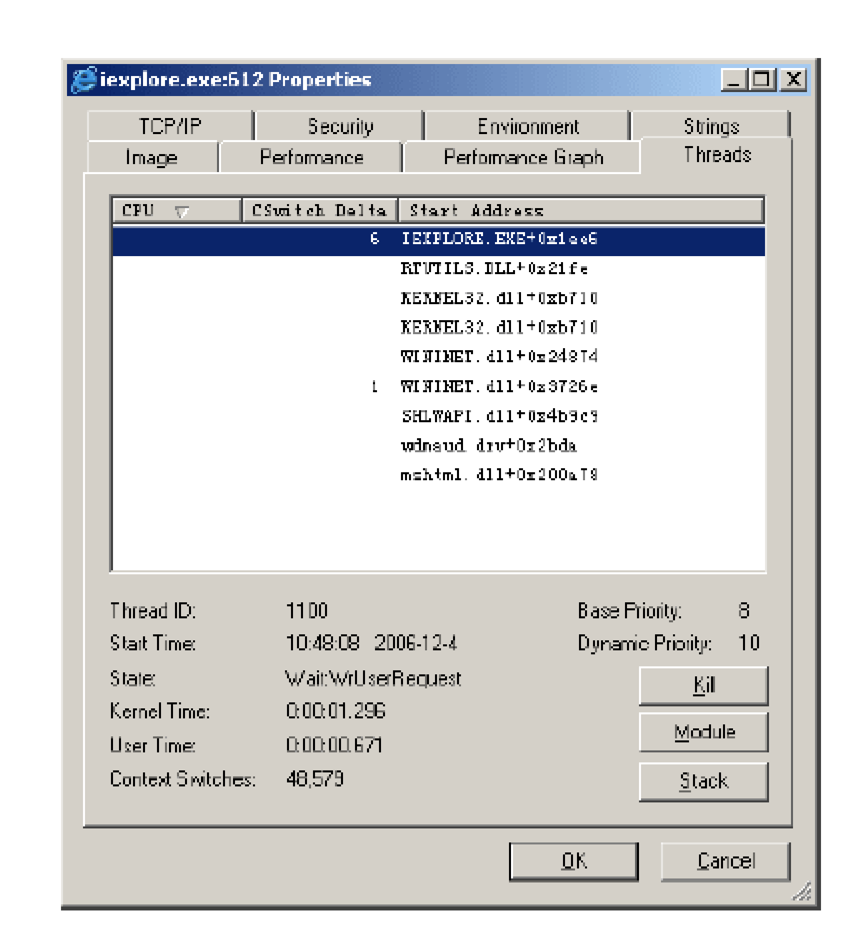



图 2-4　进程相关线程信息窗口

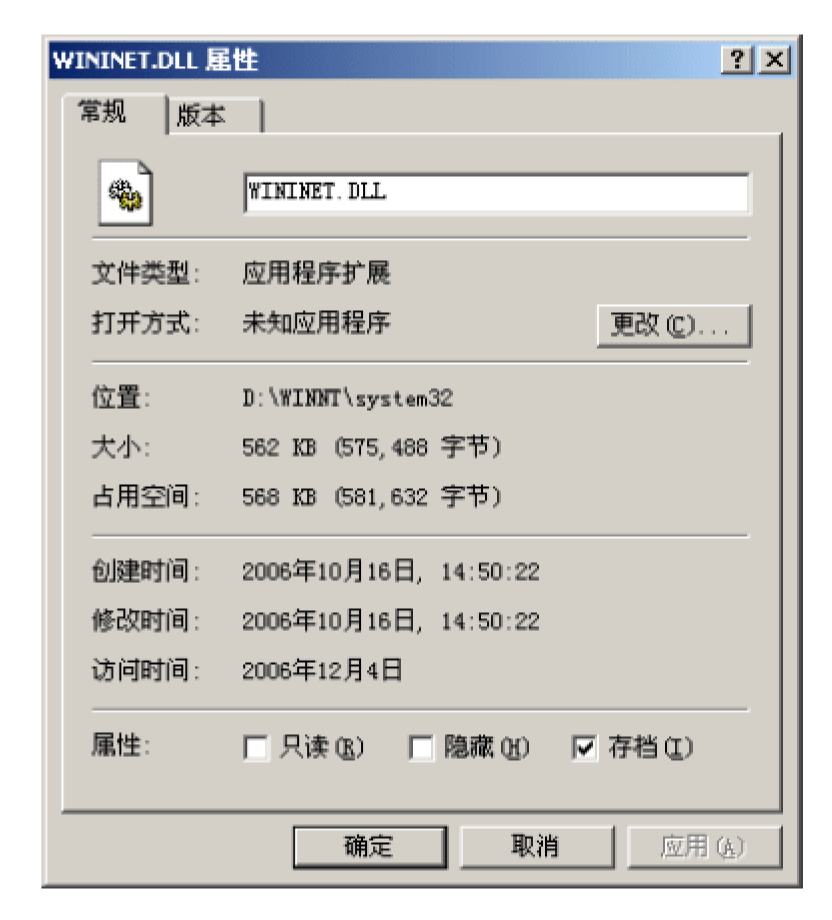


图 2-5　线程对应的文件信息

（6）查询当前引用某个动态链接库的进程，选择菜单 Find | Find Dll 命令，出现如图 2-7 所示，输入动态链接库的文件名，单击 Search 按钮，可以显示使用该动态链接库的进程列表。

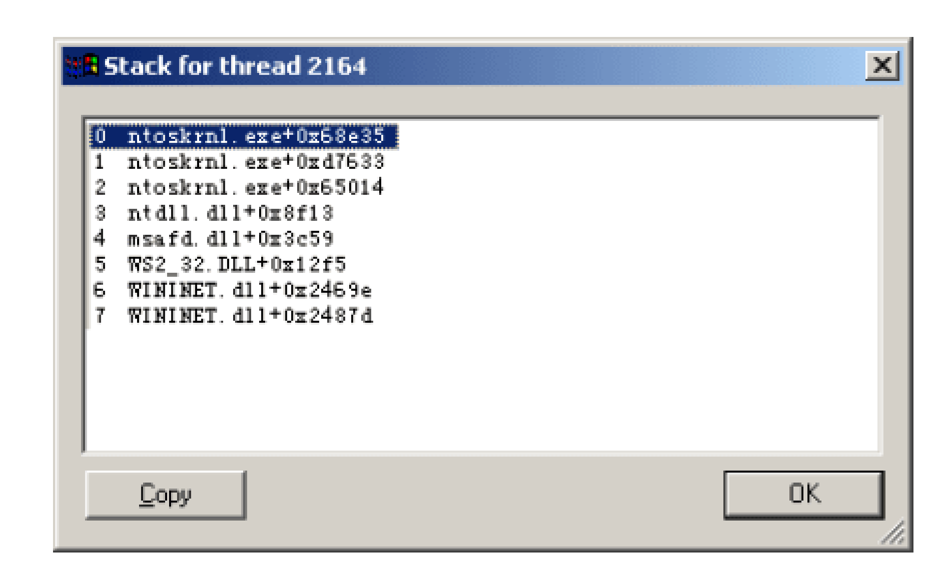


图 2-6　线程堆栈信息

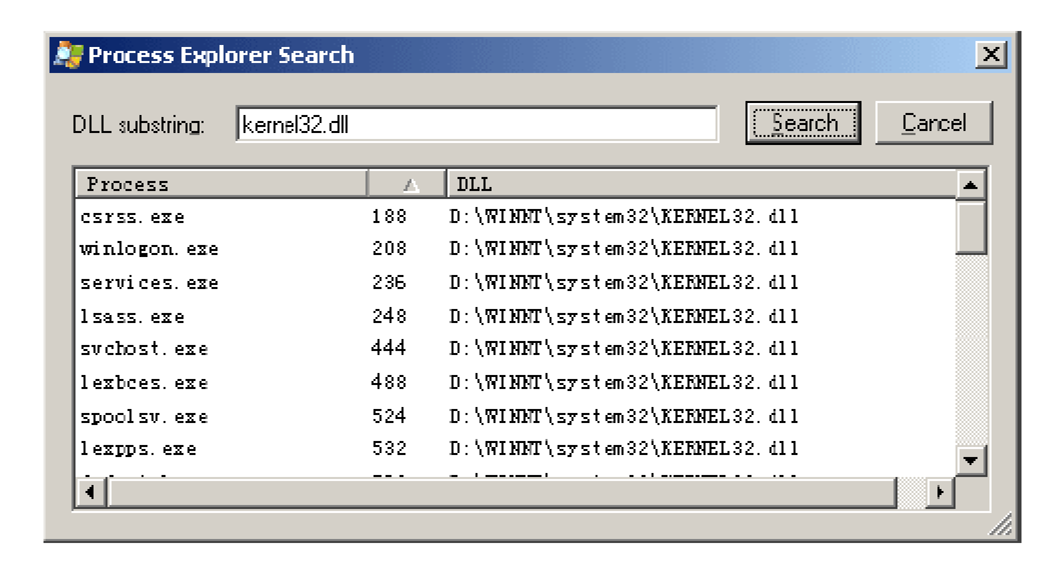


图 2-7　查询使用指定动态链接库的进程

（7）单击工具栏上的 System Information 按钮，可以查看系统的当前信息，其功能类似于进程管理器中的对应功能，如图 2-8 所示。

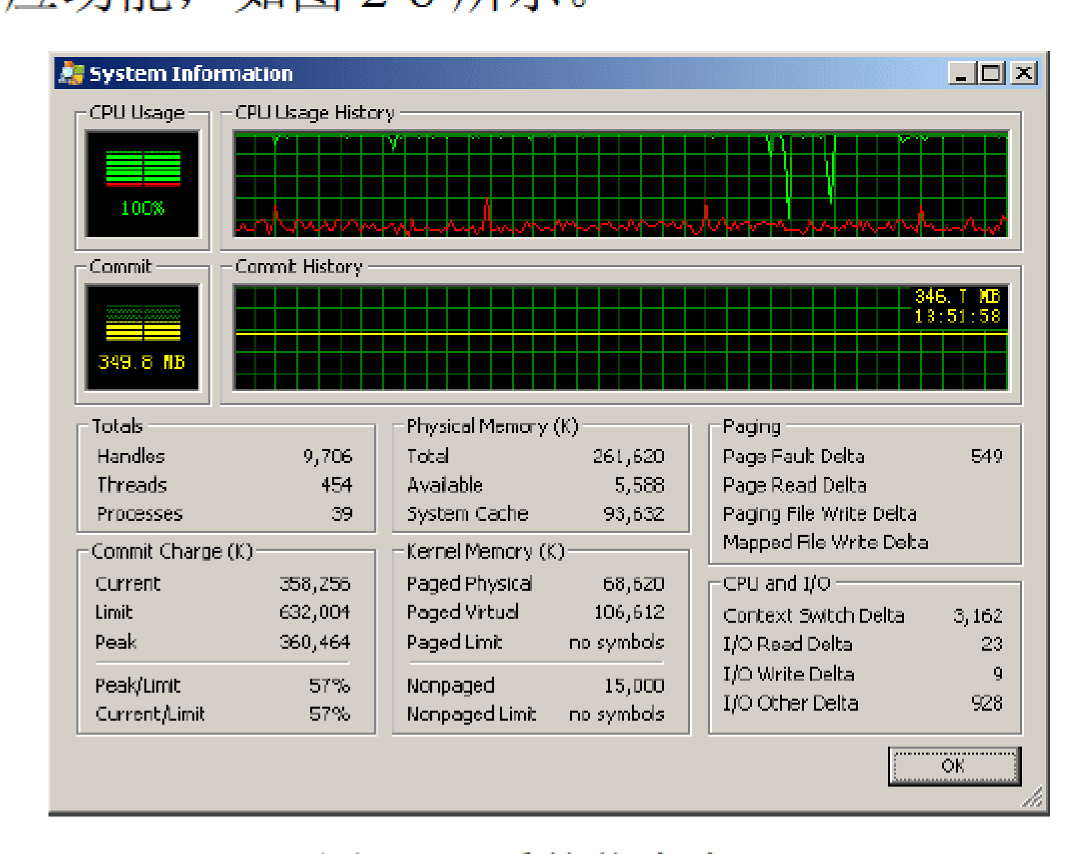


图 2-8　系统信息窗口

（8）除了上述提到的功能，该工具还有其他一些重要的功能，在此不一一讲解，希望读者自己作为练习去学习和体会。

2．自启动设置查看工具

计算机系统出现异常，通常情况下是计算机系统中运行了一些非法的进程，只要结束

这些进程就可以让系统正常运行了，而这些进程通常采取了多种措施，很难在运行状态下将其结束，此时就要考虑在计算机系统启动的过程中，不能让其运行。在 Windows 系统中，设置自动启动的地方很多，而且，不同类型的程序通常设置自动启动的位置也不相同，在此，推荐一种工具 autoruns.exe，可以很方便地发现系统中自动运行的配置，下面对其使用方法做简单介绍。

（1）找到工具程序，启动程序以后，出现如图 2-9 所示。

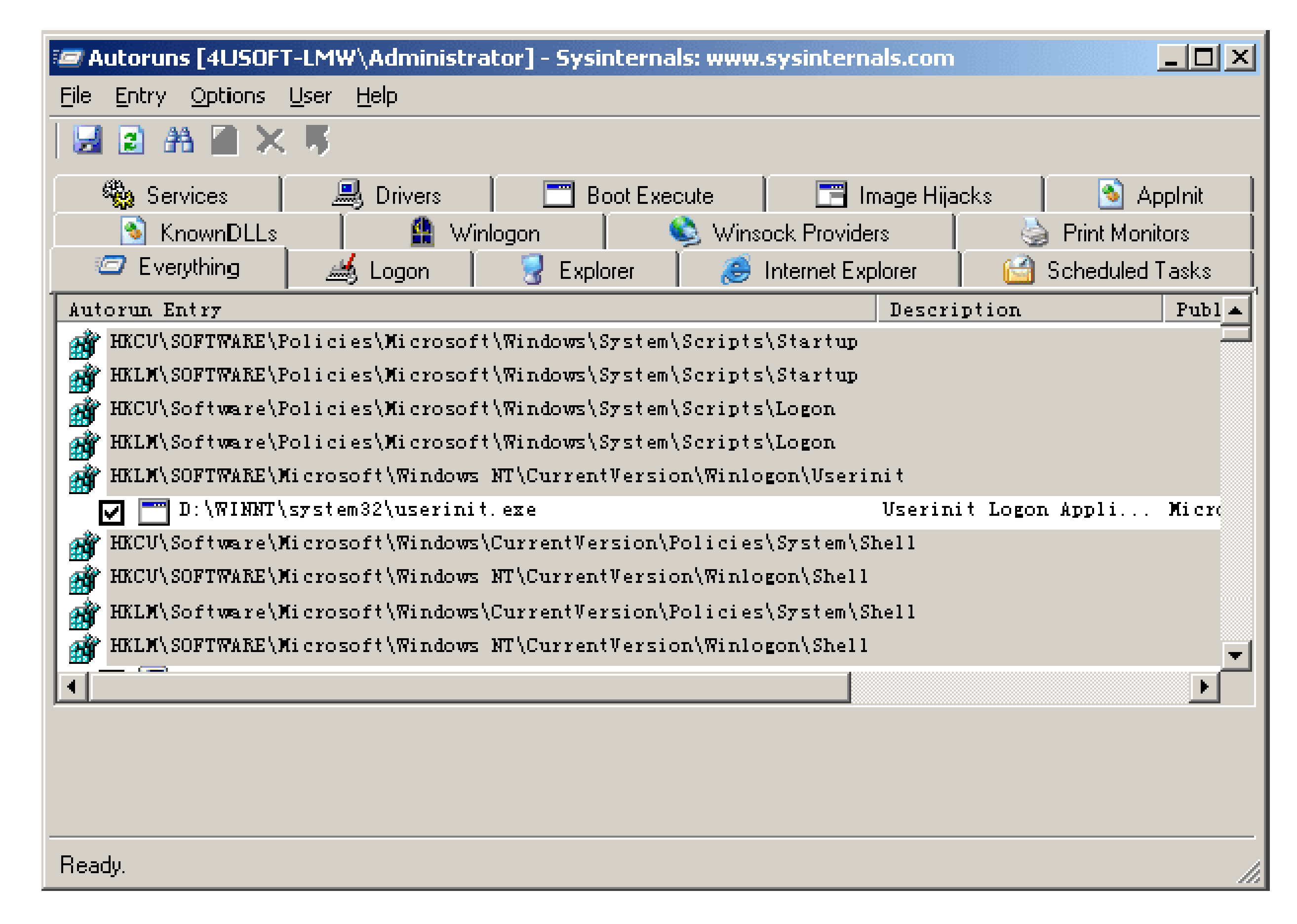


图 2-9　自启动配置查看工具

（2）通过主窗口，可以看出窗口中存在多种启动方式的配置选项卡，选择 Internet Explorer 选项卡，可以看出随着 Internet Explorer 启动的程序包括哪些，如图 2-10 所示。

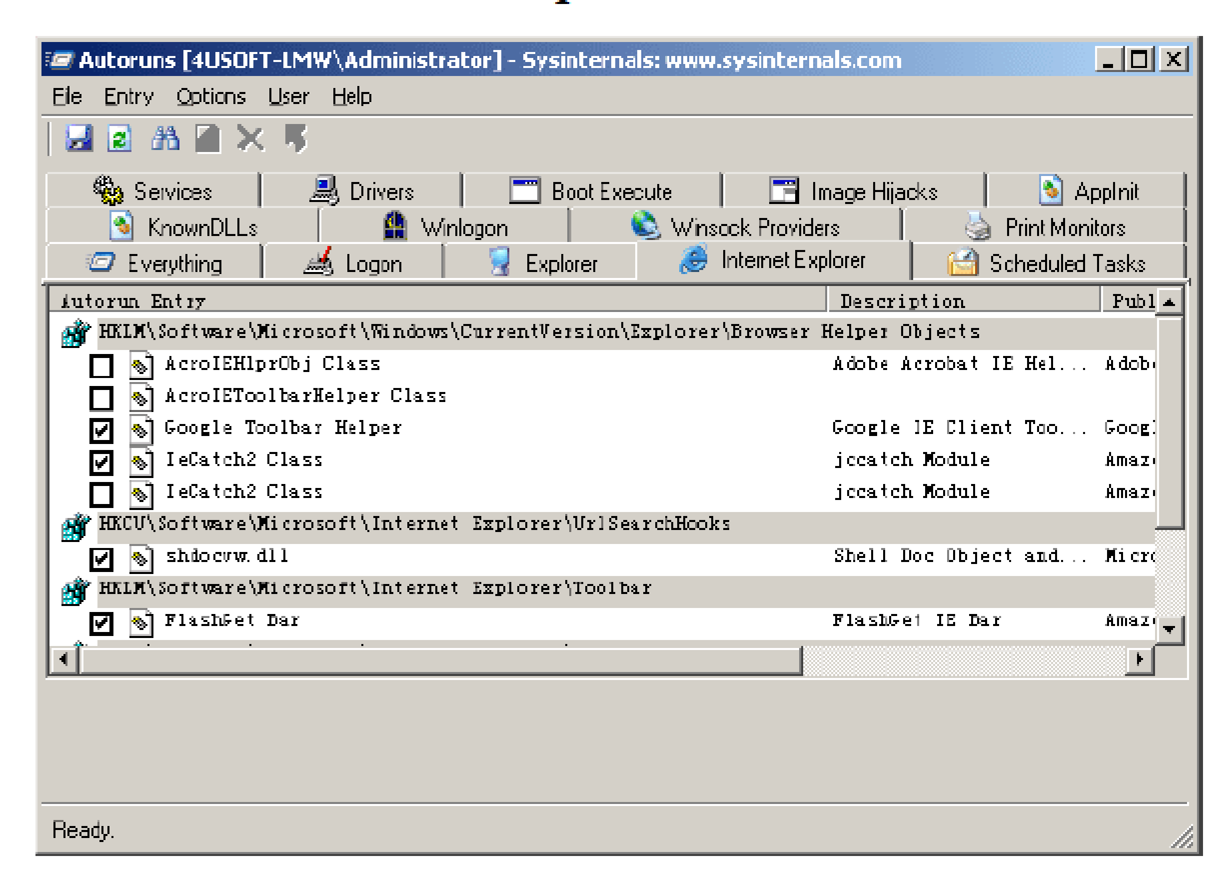


图 2-10　查看随 Internet Explorer 启动的程序

（3）在列表框中列出了多个启动项，而且还根据注册表中的位置不同进行了分类，每个启动项前面有一个复选框，如果复选框为选中状态，说明该启动项是有效的；如果复选框处于没有选择状态，说明该启动项虽然存在，但是被禁止启动了。当然，也可以通过改变复选框的状态来改变启动项的状态，即允许和禁止启动项自动启动。

（4）该工具比较简单，主要是查看是否存在非法自动启动的配置，然后通过该工具进行修改对应的设置。当怀疑有非法程序自动启动的时候，就可以用这个工具来检查。

3．通信查看工具

网络病毒的出现，使得病毒程序会通过网络与网络上的其他计算机进行通信，此时通

过通信查看程序，可以看到系统中存在的各种通信状况，在此推荐一种工具 TCPView，其使用方法如下。

（1）找到工具程序，运行程序后，其主窗口如图 2-11 所示。

图 2-11　通信查看工具主窗口

（2）在通信工具主窗口中，双击进程列表中的某个进程，可以看到进程对应的文件信息，如图 2-12，这有利于判断文件是否是合法文件，特别是文件名比较特殊的时候。

（3）主窗口列表中列举了系统中当前处于活动状态的 TCP 和 UDP 通信连接，通过右击每个列表项，可以选择结束进程或者关闭连接。

4．注册表监视工具

某些程序一旦感染病毒以后就会检测注册表，并向注册表中写入信息，特别是自启动设置，有时为了防止这些设置被修改，病毒程序会定时（比如间隔 2 秒）设置这些信息，使得手动修改这些设置机会没有用。这里推荐工具 Regmon.exe。下面对其使用方法简单介绍。

（1）找到工具程序文件，运行程序，出现如图 2-13 所示。

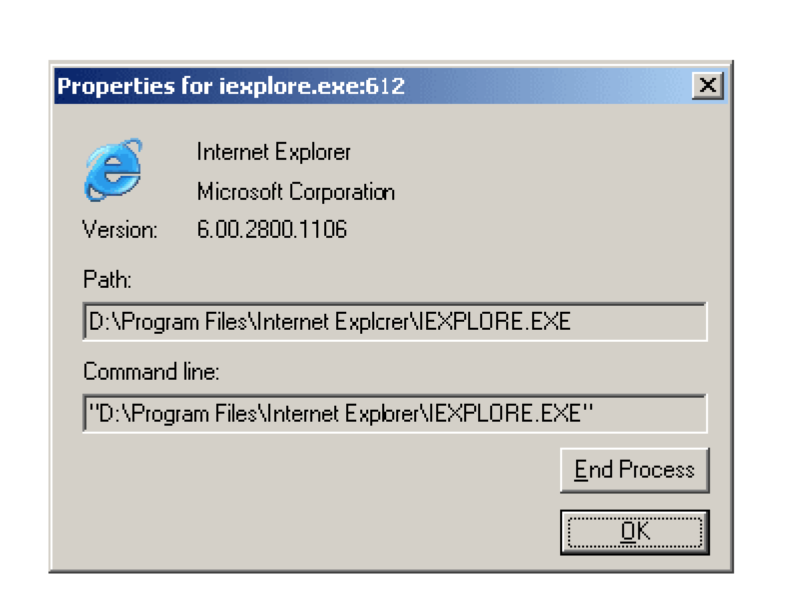


图 2-12　进程位置信息

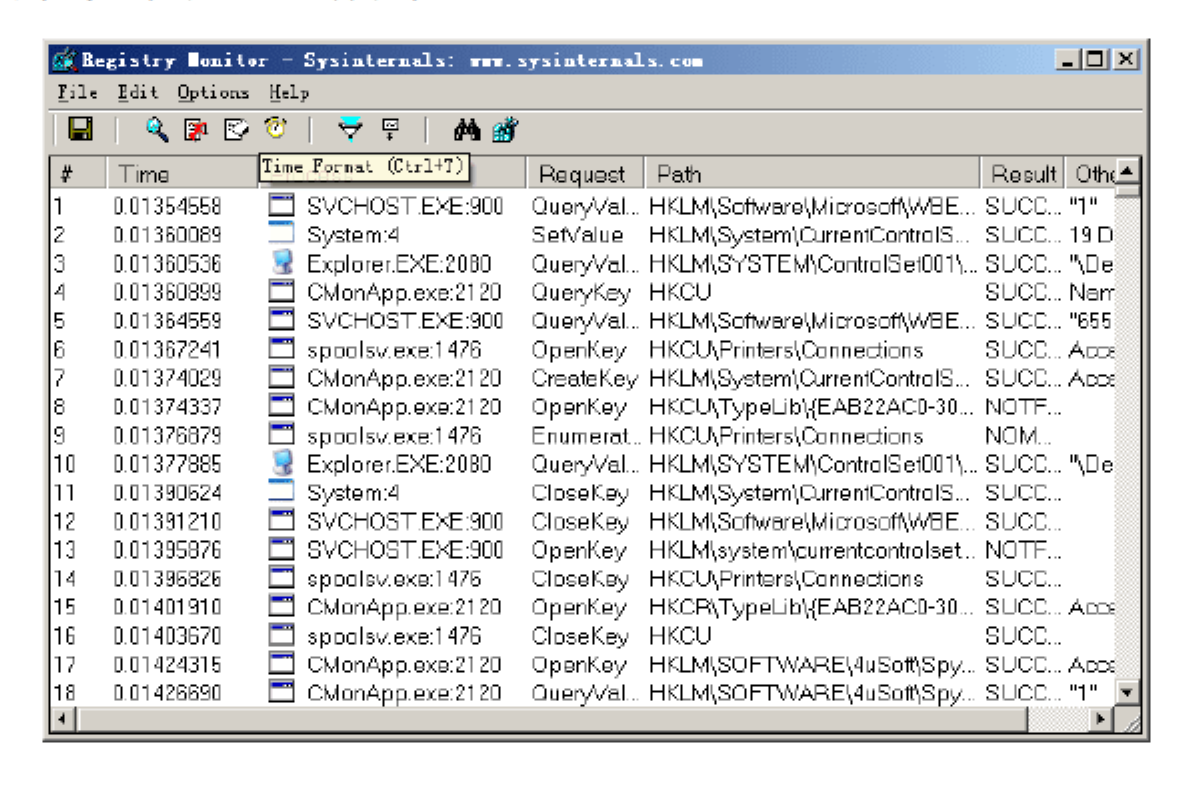


图 2-13　注册表监视工具窗口

（2）系统中存在多个程序需要访问注册表，利用这个工具可以对这些访问操作进行记录，当然，并不是所有的信息都需要，往往只是需要监视某个特定的注册表键。此时可以通过对过滤器设置来达到这个目的，单击工具栏上的过滤器按钮，出现如图 2-14 所示。

（3）在过滤器设置窗口中，可以设置需要查看记录的条件，方法是：在 Include 下拉

列表框中输入需要包含的字符，或者在 Exclude 下拉列表框中输入不包含的字符，或者在 Highlight 下拉列表框中输入需要亮显示的字符，单击 OK 按钮，使设置生效。

5．调试信息查看工具

使用调试信息查看工具查看异常信息也是常用方法之一，因为在开发程序（包括正常程序和病毒程序）时，为了保证程序能够正常运行，都会对程序进行调试，这个工具对调试程序是非常方便的，工具名称为 DebugView，下面对其用法简单介绍如下。

（1）找到工具程序，启动程序，工具主窗口如图 2-15 所示。

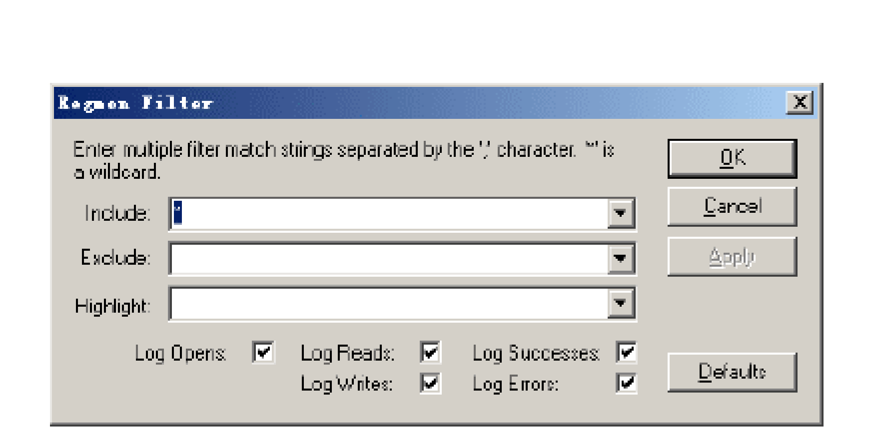


图 2-14　注册表监视工具过滤器设置窗口

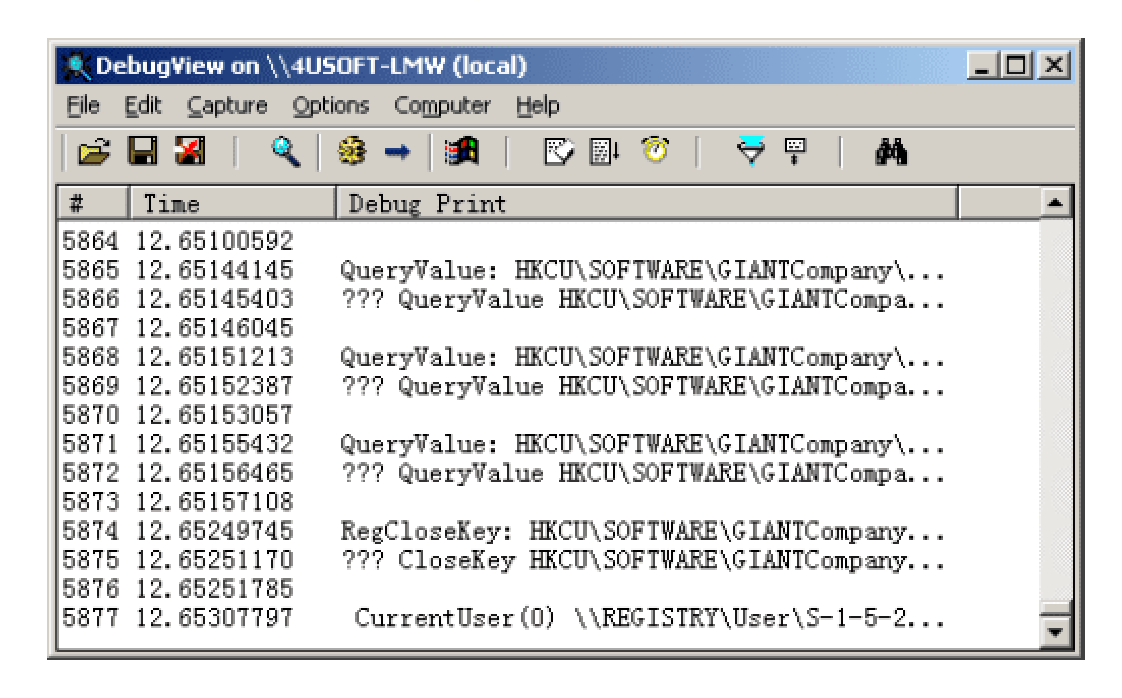


图 2-15　调试信息查看工具

（2）因为系统中通常存在多种程序会输出调试信息，所以这里显示的消息可能会非常多，同样，这些信息并不都是有用的，通常只要少数特定的信息才有用，所以需要对信息进行过滤，即设置过滤器。单击工具栏上的过滤器设置按钮，出现如图 2-16 的窗口。

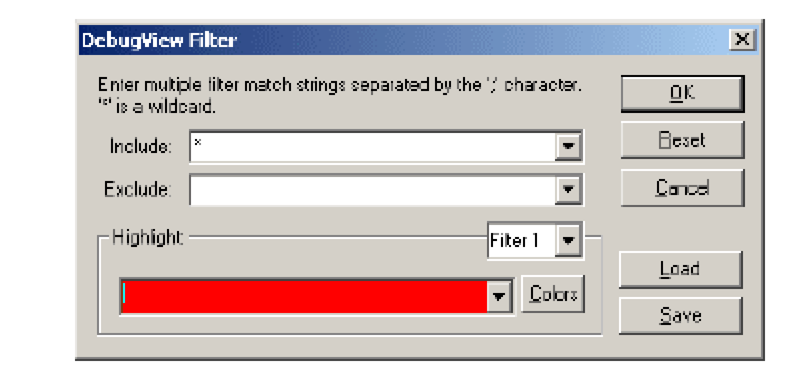


图 2-16　调试信息查看工具过滤器

（3）在过滤器设置窗口中，在 Include 下拉列表窗口中可以设置符合条件的记录应该包含什么字符，如果设置为“*”，表示显示全部记录；在 Exclude 下拉列表窗口中可以设置不能包含的字符，设置完成，单击 OK 按钮，使设置生效。

（4）该工具比较简单，除了上面介绍的功能以外，还有一些方便的功能，希望读者作为练习认真体会。

6．文件监视工具

有时通过各种工具发现计算机上存在某个非法文件，想方设法将其删除以后，马上该文件又出现了，此时有必要对文件操作情况进行监视，这里推荐一款工具为 FileMon，可以监视系统对文件的各种操作，有利于发现是什么程序创建的文件，对彻底解决非法程序有很大的帮助。

（1）找到工具程序，运行程序，出现如图 2-17 所示。

（2）系统对文件操作每时每刻都在进行，所以也会存在大量的文件操作记录，同样，绝大部分记录都是没有意义的，只有找到与特定文件有关的记录才有价值。工具同样提供了过滤器设置。单击工具栏上的过滤器设置按钮，出现如图 2-18 所示窗口。

（3）过滤器设置与调试过滤器设置基本是一致的，在此不再详细叙述。读者对该系统工具多进行实践操作，以便在必要的时候能够熟练利用。

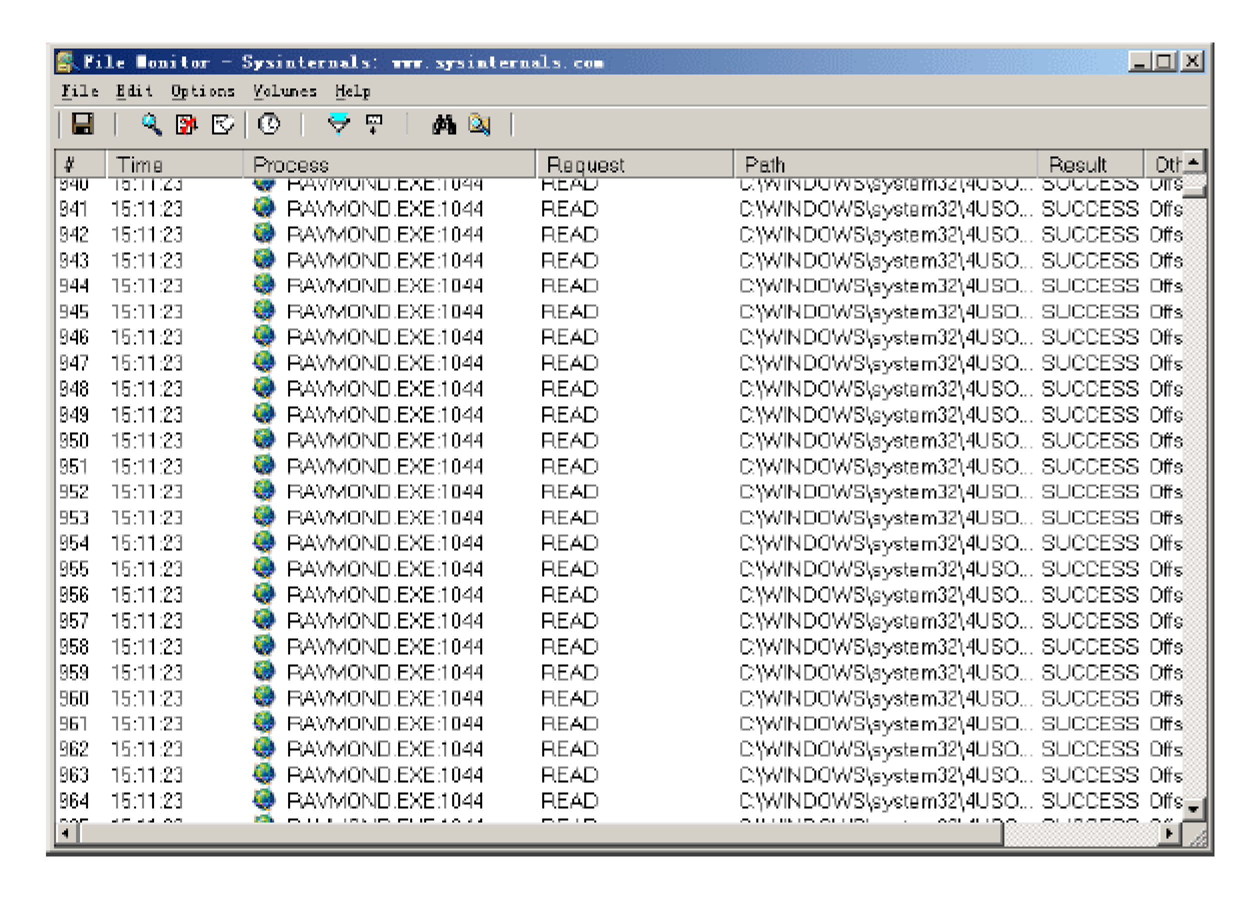


图 2-17　文件监视工具

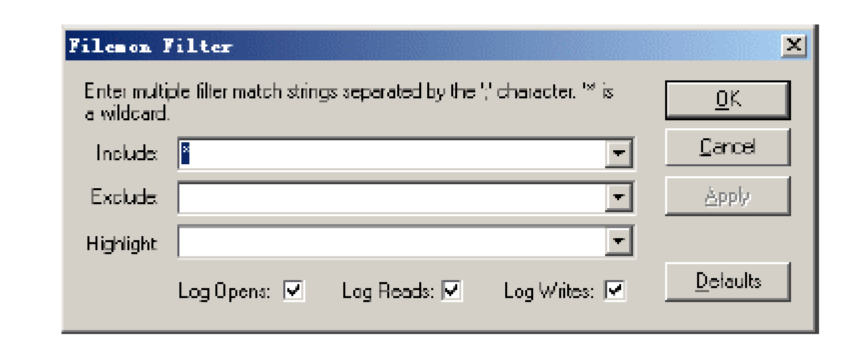


图 2-18　文件监视工具过滤器

2.3.2　手动清除飘雪病毒

当计算机系统感染飘雪病毒后，IE 的主页会被修改为“http://www.piaoxue.com”，而且每过一会儿就会弹出一个网页窗口，同时让系统变慢，下面对该病毒做相关分析，并就手工清除该病毒的过程进行说明。

1．病毒感染过程分析

病毒感染的时候，首先检查该计算机有没有被感染，判断的方式是通过检查系统中是否存在注册表键 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer \SearchPlugInX），如果存在，就不再感染，所以可以根据这一点来免疫。

检查系统中是否安装了虚拟机，判断方式是通过检查是否存在注册表键 HKEY_LOCAL_MACHINE\Software\Vmware,inc.\Vmware Tools，如果存在，则直接退出。这点主要是防范系统调试人员，如果在虚拟机上安装，就退出。

该病毒没有采用 BHO 的方式来完成自己的自动启动，而是通过驱动程序的方式来完成自动启动的，病毒程序感染时会随机生成两个驱动文件，文件名称是随机生成的，不同的计算机感染时，驱动文件名称不相同，但是两个文件名称都是 8 个字符，然后将驱动文件复制到%system%\system32\drivers 目录下，并将驱动安装到系统中。安装的过程生成 eugnxqcx.sys 和 wllcnlke.sys。

2．使用工具进行分析

当病毒运行以后，会建立两个系统线程，使用进程查看工具找出这两个系统线程，具体步骤如下：

（1）启动进程查看工具，选择 System 进程，如图 2-19 所示。

（2）双击 System 进程，在弹出的窗口中选择 Thread 选项卡，如图 2-20 所示。

（3）可以看到线程列表中最后两个线程。这两个线程一直不停地检查注册表键 HKLM\SYSTEM\CurrentControlSet\Services\下这个驱动的值，如果删除马上又会生成。这两个线程虽然看到但是没有办法杀掉，会提示没有权限。

3．清除方法

前面谈到该病毒的启动方式是通过驱动的方式来启动的，那么首先要找到对应的驱动程序启动配置，具体步骤如下。

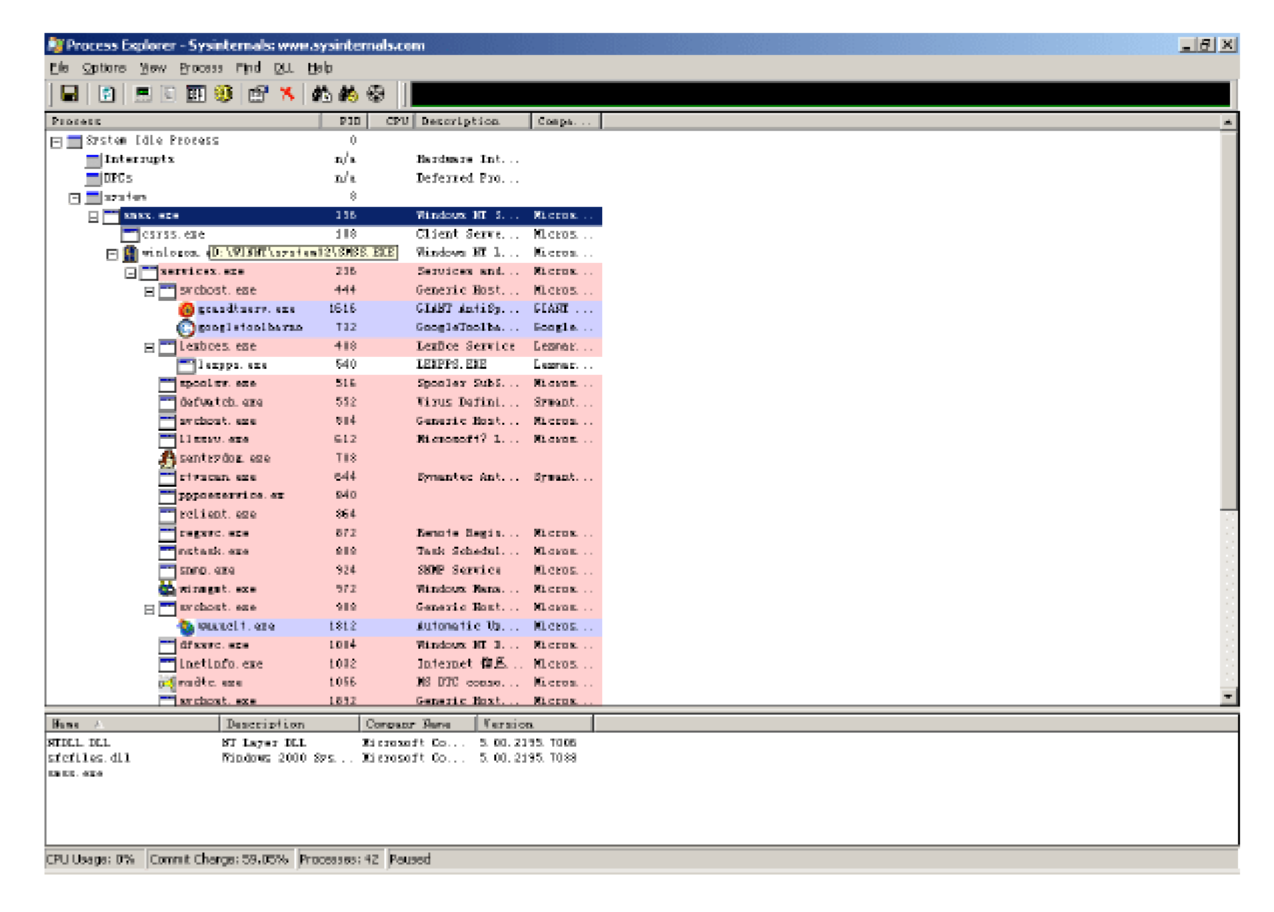


图 2-19 Process Explorer 窗口

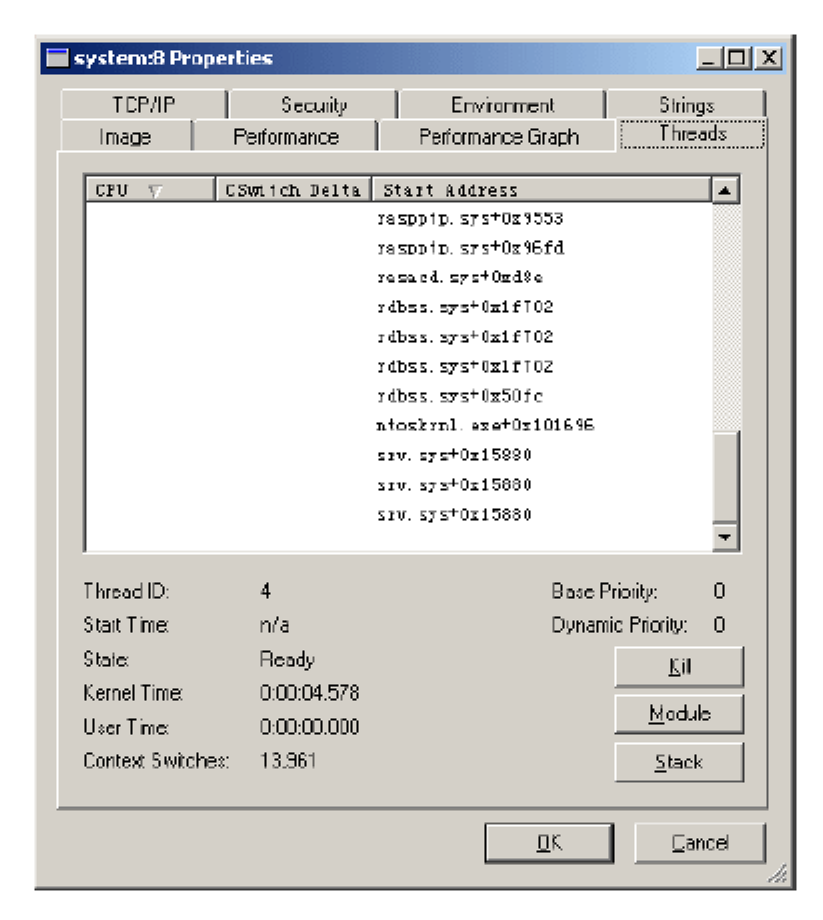


图 2-20 System 进程的线程信息

（1）运行自启动设置查看工具 Autoruns，如图 2-21 所示。

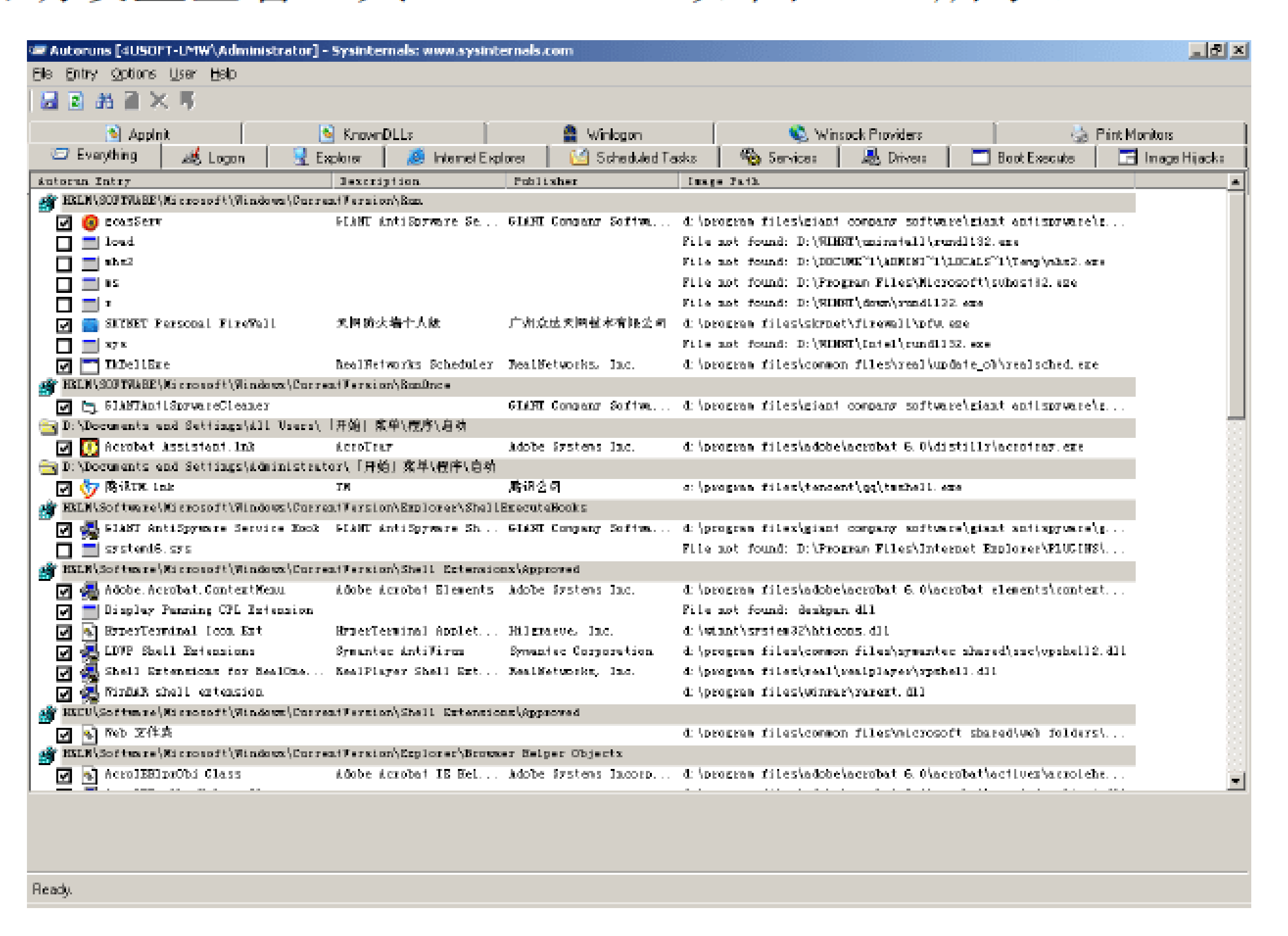


图 2-21 自启动查看工具

（2）选择菜单 Options | Code Signatures（验证代码签名）命令和 Hide Signed Microsoft Entries（隐藏已签名的微软项）命令，然后按 F5 键，重新获取启动信息，单击窗口上的 Driver 选项卡，显示没有得到微软签名的驱动启动项，如图 2-22 所示。

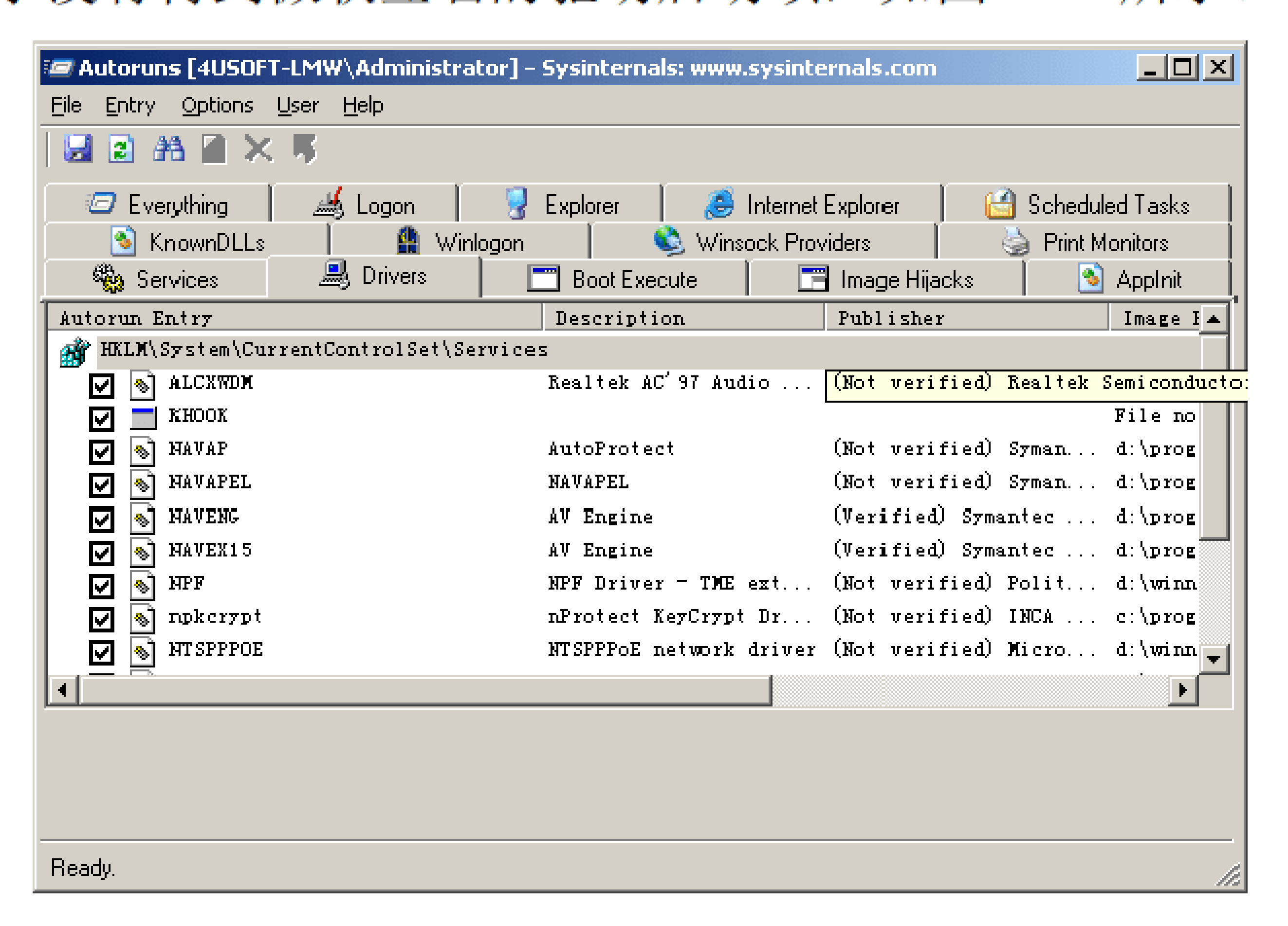


图 2-22 自启动的驱动设置

（3）可以通过驱动名称、驱动描述、驱动开发商以及驱动文件的位置和驱动文件名称来判断出病毒所安装的驱动，然后将驱动项前面的复选框取消选择即可。

找出驱动文件的位置和名称了，但是此时还不能对这两个文件进行删除，因这两个文件正在被系统使用，下面是删除文件的步骤。

提示： 进行此项操作前首先选择 Process Explorer 窗口上的 View | Show Lower Pane 命令，使其处于选择状态，然后选择 View | Lower Pane View | Handles 命令，使其也处于选择状态。

（1）在 Process Explorer 中，选择 Find | Find Handle 命令，出现如图 2-23 所示对话框，在 Handle or Type 文本框中输入刚才发现的驱动文件名称。

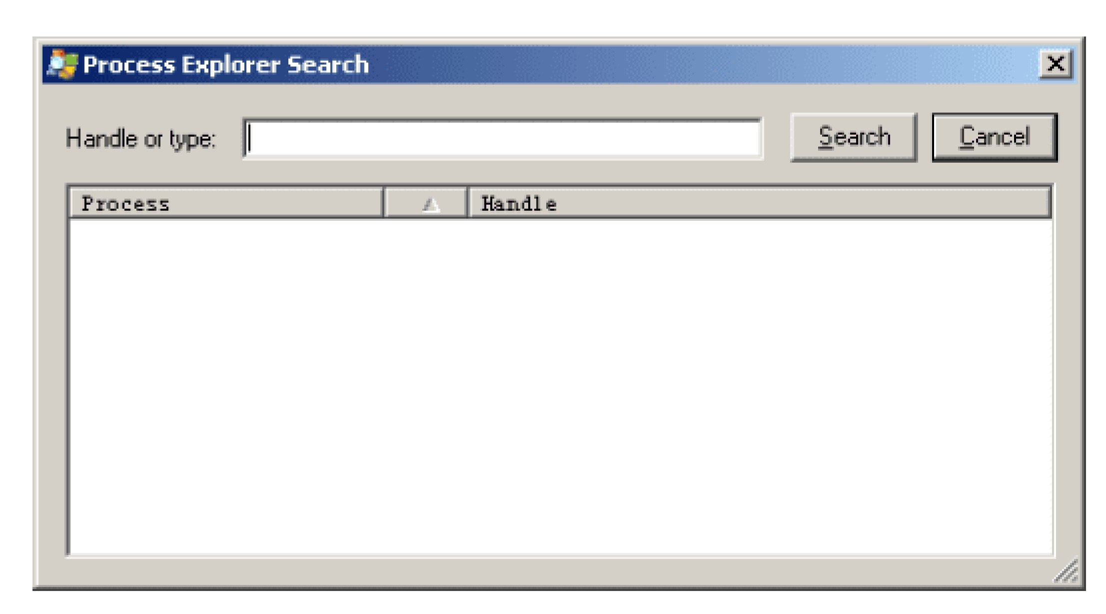


图 2-23　查找线程句柄

（2）单击 Search 按钮，即可找到依附于 System 进程的病毒线程，找到病毒线程对应的 Handle，如图 2-24 所示，右击该项，然后从弹出的菜单中选择 Close Handle，该线程就被停止了。

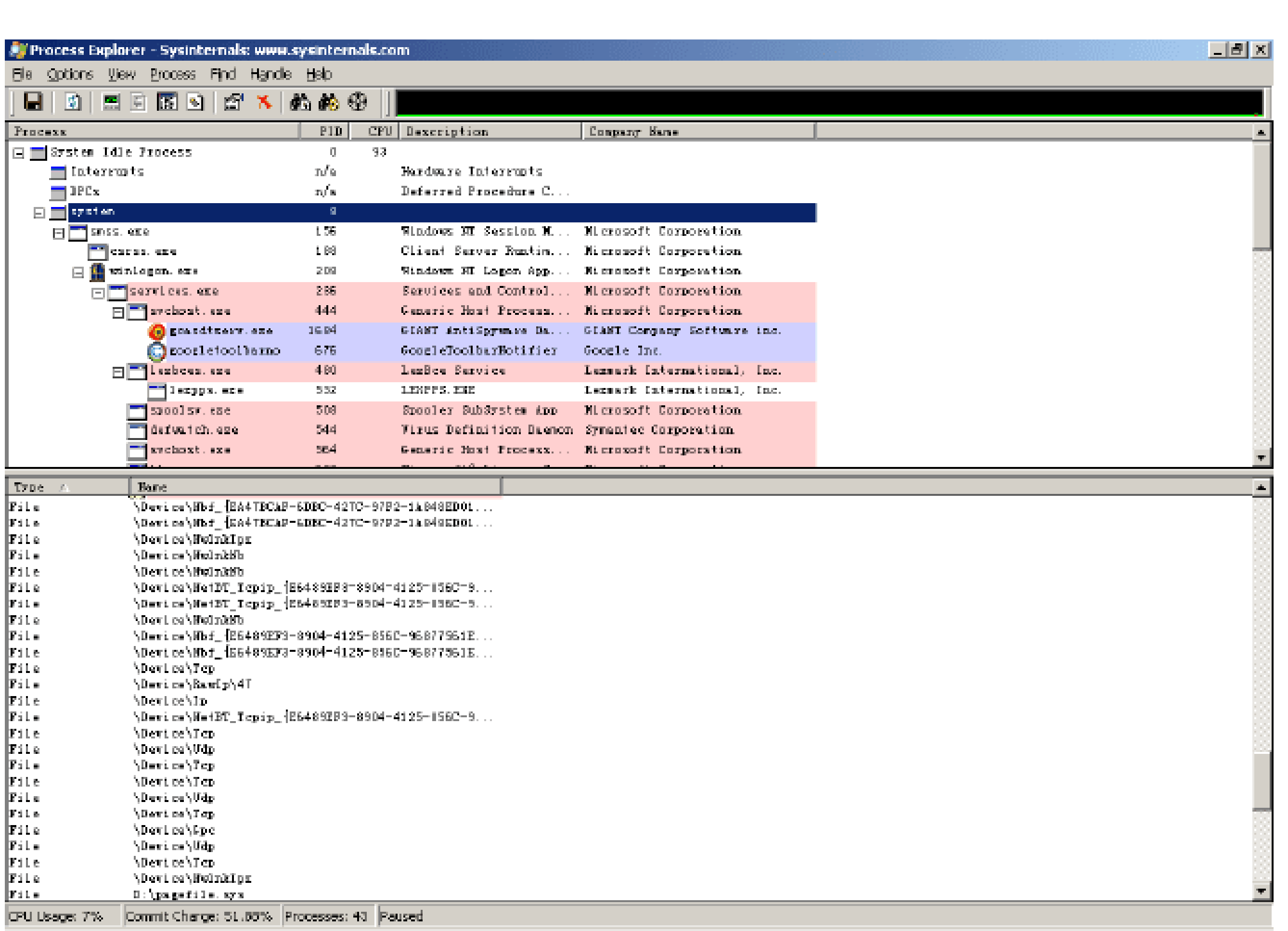


图 2-24　System 进程句柄

（3）打开资源管理器，找到病毒文件的位置，将病毒文件删除，这样就完成对飘雪病毒的手工清除了。

提示： 手工清除病毒的几个基本步骤通常是首先用进程查看工具（Process Explorer）检查一下，看看有什么异常的进程，然后用自启动设置查看工具（Autoruns）检查，看有什么非法进程被添加到启动项了，通过这两种方法可以查看常见的木马病毒。

2.4 计算机病毒防范措施

计算机病毒防范措施主要包括两个方面的内容。一是计算机病毒的预防，即尽量避免计算机系统被病毒感染，以及在计算机病毒未造成任何破坏之前将其清除；另一个是当计算机病毒造成破坏时，要能够及时采取补救措施，将损失减小到最低并总结经验，为计算机病毒预防提供帮助。

2.4.1 计算机病毒的预防

解决计算机病毒问题的最有效方法是采取积极有效措施，防止被计算机病毒所感染，为了达到这一目的，可以采取如下措施。

1. 备份重要数据

病毒出现是很难预测的，而且杀毒软件也不能保证杀掉所有的病毒。平时辛辛苦苦写的论文，编的程序，找的资料，公司的账目等等，总不希望突然被病毒所毁。所以要确保资料安全，备份是很重要的。况且，备份时要根据需要备份内容的大小选择合适的备份媒体，比如只有几十兆的资料可以采用优盘，几百兆的文件资料可以选择刻录光盘或者硬盘备份。不过，在备份前要确定资料是完好而且无病毒的。

备份数据需要根据数据的特点来进行安排，对于不会频繁变动和使用的数据，采用刻录光盘的方式来备份比较合适，而且备份的次数也会较小，对于需要经常变动和使用的文件，通常采用可读写的硬盘来备份，因为这样使用的时候非常方便。如果备份的数据量比较小（包括文件大小和文件数量）时，可以通过复制粘贴的方式来备份，如果需要备份的数据量比较大，最好的方式就是选择专门的备份工具软件，还有对于特别重要的计算机系统，还可以采取双硬盘备份，当其中某一块硬盘损坏时，另一块硬盘可以保证系统中数据的完整性。

提示：数据备份需要根据具体情况进行分析，选择最简单、有效的备份方式，确保数据安全，在特殊情况下，可以考虑采用光盘、硬盘等多种方式进行，还要养成经常备份的习惯。

2. 安装杀毒软件及防火墙

安装杀毒软件和防火墙对于预防病毒是十分重要的，虽然不能保证百毒不侵，但是也可以让计算机运行得比较放心。杀毒软件不宜安装多个，多个杀毒软件易出现冲突，而且占用系统资源，对于系统来说反而有弊而无利。防火墙要设置好，有些防火墙，防止外面不明数据流入的确很有效，但是设置不当，会造成有些程序不能访问网络，如有些不能进行网络视频，不能传输文件，不能玩游戏，甚至会造成有些网址不能访问。设置好防火墙相应的参数才能让网络生活更加丰富，但是防火墙允许更多的程序访问网络，就相当于对网络开放更多的端口，那样病毒更容易入侵，所谓有得必有失，应该根据实际情况而定。不可能把计算机的全部端口都封掉——那样的话的确病毒进不了，但是也访问不了计算机网络，另外，杀毒软件和防火墙一定要记得经常升级更新，那样才能应付大部分新出的病毒。

> 提示：杀毒软件和防火墙是计算机安全的两个最基本的措施，当计算机系统安装完成的时候，首先就应该安装这两种软件，条件允许还应该安装反间谍软件，然后才能将计算机接入到网络，进行系统升级，只有将这些基本的安全措施做好以后，才能浏览网页。

3．为系统打上补丁

系统漏洞让病毒更容易入侵，因此，系统软件官方网站提供了很多漏洞补丁，其实装系统的时候就应该马上补上系统补丁，否则，访问网络将会很容易染上病毒。

> 提示：Windows 操作系统安装完成后，需要做的一件重要事情就是连接到 Windows 的补丁网站打补丁，这样才能保证操作系统中已经发现的漏洞被修复，大大减小受到网络攻击的可能性，对于一台新安装的计算机，在没有采取任何安全措施的情况下，只需要几分钟的时间就会受到攻击，关于为操作系统打补丁的操作方法和步骤请参考第 5 章第 5.1.1 节系统补丁的相关内容。

4．及时关注流行病毒以及下载专杀工具

因为很多流行病毒和特殊病毒的存在，为了网络安全以及及时防止病毒的扩展，很多杀毒软件商官方网站都免费提供专杀工具。有些病毒是普通杀毒软件不行而需要专杀工具才行的，因此我们必须经常留意官方所公布的新种类病毒以及下载相应的专杀工具。

> 提示：当计算机感染病毒，使用计算机上的杀毒工具扫描，却没有发现病毒时，可能是计算机病毒库需要更新才能查杀该病毒，或者该杀毒软件不能识别当前感染的病毒（即使将病毒库升级到最新），此时需要查找病毒专杀工具。

5．注意使用计算机时候的异状

有时候使用着计算机，会突然内存占用很高，或者 CPU 使用率很高，或者资源（指内存和 CPU）使用情况忽高忽低，那么就很可能是感染病毒了，那么就要注意了。

对于 Windows 2000 和 Windows XP 以及 Windows 2003 可以通过查看任务管理器，结束不明进程（Windows 98 和 Windows Me 可以通过 Ctrl+Alt+Del 查看和结束不明进程）；有时病毒还会开机自启，有些可以通过输入命令 msconfig 打开系统配置使用程序，管理开机运行程序（注：Windows 2000 没有 msconfig，但是可以从其他系统复制过来用），让病毒不能开机自启。

6．注意局域网共享安全

共享文件最好设置密码和只读。假如不是只读，那么网络上病毒侵入您的计算机将更加容易，密码也可以有效保护您的资料不轻易被他人所取得。

7．注意网页邮件病毒

装了杀毒软件，也要注意网页上的病毒，毕竟没有一种杀毒软件是万能的。上不明网站，经常有病毒及恶意代码，修改 IE 主页，甚至上不了网，这种现象是很多人都碰到过的。目前，不少杀毒软件和系统优化软件都有修复 IE 功能。很多病毒也是会通过邮件传播的，因此，我们不能随便下载邮件中的不明附件，因为往往病毒就隐藏在附件当中。即使朋友寄来的附件下载了也要通过杀毒软件扫描过才能打开。

8．注意定期扫描系统

虽然可能经常开着杀毒软件，或者杀毒软件开着时没发现问题，只是意味着当前运行程序中没有病毒，也就是病毒没有发作，但是并不是说计算机上就没有病毒。假如计算机上有病毒，即使不发作，那也很可能在您的文件传输中，共享等过程中传染给别人，而且当时病毒不发作，可能以后就很容易发作，所以，为了保证系统安全，就要定期扫描系统。

系统没有绝对的安全，只有重视病毒预防，计算机才能处于相对的安全之中。而且，对于经常有工作资料和其他重要资料在计算机上的用户，备份是十分重要的。

提示： 定期对系统进行病毒扫描是及时发现并防范计算机病毒的重要方法之一。因为计算机病毒的隐蔽性，在计算机病毒未发作以前对系统几乎没有影响，也不容易被察觉到，所以在此时通过扫描将病毒杀掉即可避免病毒造成的损失。

2.4.2　计算机病毒感染后的一般修复处理方法

一旦遇到计算机病毒破坏了系统也不必惊慌失措，采取一些简单的办法可以杀除大多数的计算机病毒，恢复被计算机病毒破坏的系统。

下面介绍计算机病毒感染后的一般修复处理方法。

（1）首先必须对系统破坏程度有一个全面的了解，并根据破坏的程度来决定采用有效的计算机病毒清除方法和对策。

如果受破坏的大多是系统文件和应用程序文件，并且感染程度较深，那么可以采取重新安装系统的办法来达到清除计算机病毒的目的。而对感染的是关键数据文件，或比较严重的时候，比如硬件被 CIH 计算机病毒破坏，就可以考虑请防杀计算机病毒专家来进行清除和数据恢复工作。

（2）修复前，尽可能再次备份重要的数据文件。

目前防杀计算机病毒软件在杀毒前大多都能够保存重要的数据和感染的文件，以便能够在误杀或造成新的破坏时可以恢复现场。但是对那些重要的用户数据文件等还是应该在杀毒前手工单独进行备份，备份不能做在被感染破坏的系统内，也不应该与平时的常规备份混在一起。

（3）启动防杀计算机病毒软件，并对整个硬盘进行扫描。某些计算机病毒在 Windows 95/98 状态下无法完全清除（如 CIH 计算机病毒），此时我们应使用事先准备的未感染计算机病毒的 DOS 系统软盘启动系统，然后在 DOS 下运行相关杀毒软件进行清除。

（4）发现计算机病毒后，我们应利用防杀计算机病毒软件清除文件中的计算机病毒。如果可执行文件中的计算机病毒不能被清除，一般应将其删除，然后重新安装相应的应用程序。

（5）杀毒完成后，重新启动计算机，再次用防杀计算机病毒软件检查系统中是否还存在计算机病毒，并确定被感染破坏的数据确实被完全恢复。

（6）此外，对于杀毒软件无法杀除的计算机病毒，还应将计算机病毒样本送交防杀计算机病毒软件厂商的研究中心，以供详细分析。

2.4.3　诺顿杀毒软件

为了理解杀毒软件的功能以及使用杀毒软件的方法，在此以诺顿杀毒软件为例来说明杀毒软件的使用方法。

> **提示：**没有任何一种杀毒软件可以杀掉所有的计算机病毒，因为计算机病毒千变万化，而且不断有新的病毒加入，所以当发现计算机出现感染病毒症状时，可以首先选择一种杀毒软件来进行杀毒。如果没有发现病毒，并不等于计算机没有感染病毒，可以换一种杀毒软件来进行杀毒，即使杀掉了一些病毒，如果计算机还是有感染病毒症状时，还需要换其他的杀毒软件进行杀毒，或者通过症状查询相关信息，有时比较新的病毒可能使用一些专杀工具效果会比较好。

1．杀毒软件升级

程序的具体操作如下。

（1）选择“开始”|“程序”| Symantec Client Security |“Symantec Antivirus 客户端”命令，出现如图 2-25 所示。

（2）单击窗口右边的 LiveUpdate 按钮，出现 LiveUpdate 对话框，如图 2-26 所示。

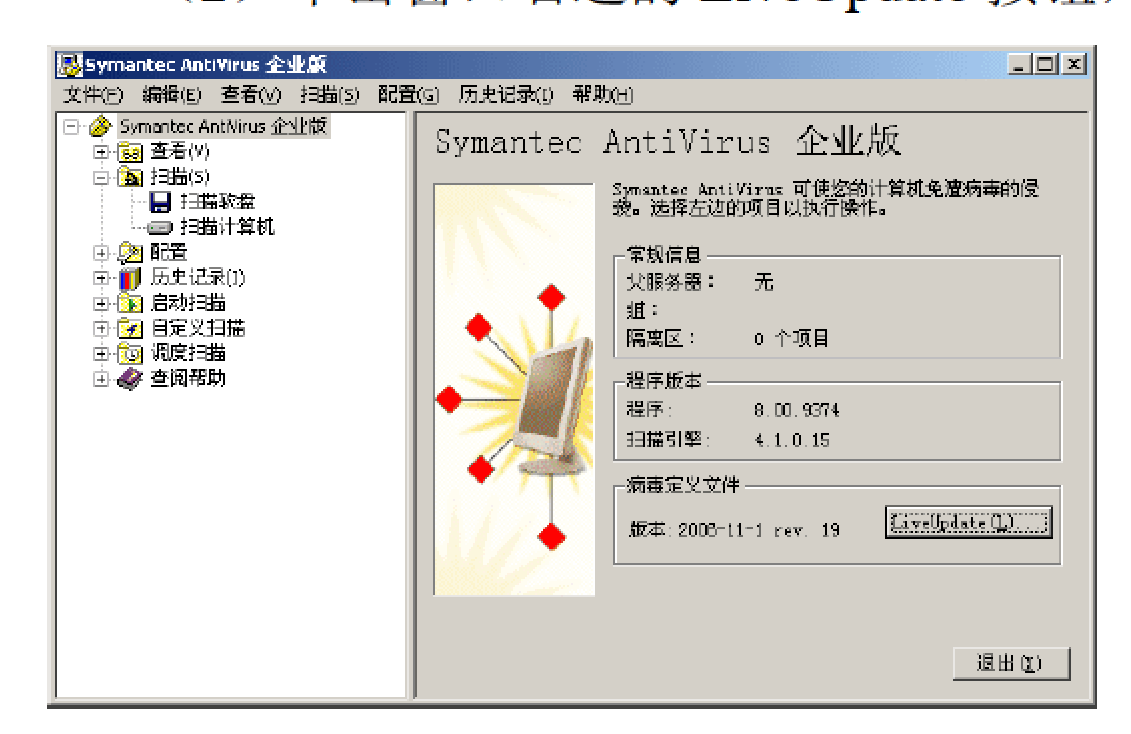


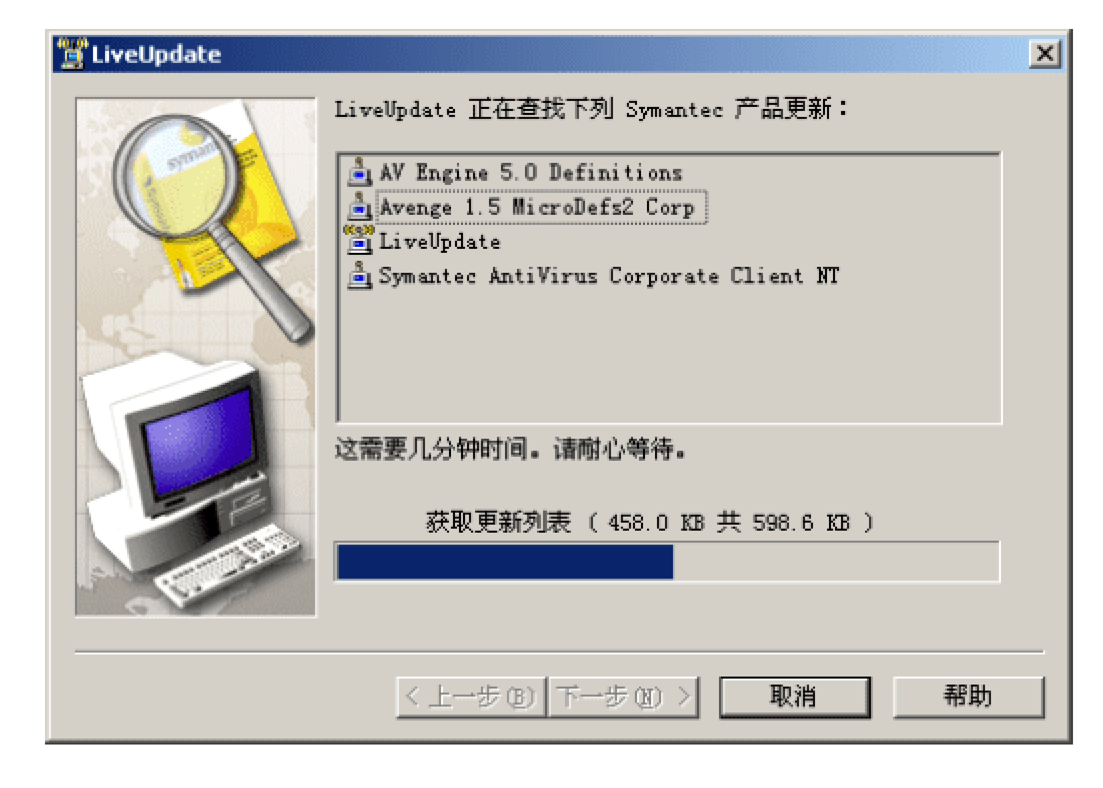
图 2-25　诺顿杀毒软件界面



图 2-26　LiveUpdate 对话框

（3）单击“下一步”按钮，系统开始下载升级程序，如图 2-27 所示。

（4）升级程序下载完成以后，出现下载完成提示窗口，如图 2-28 所示。



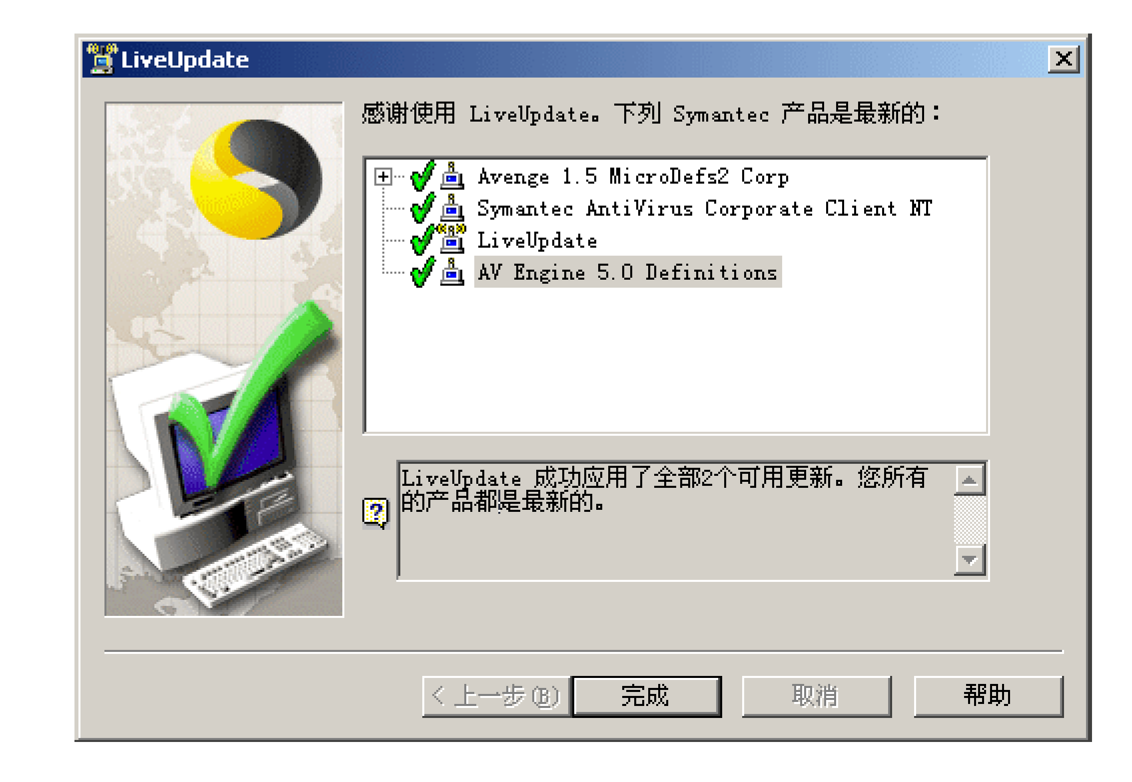




图 2-27　下载升级程序窗口　　图 2-28　完成升级程序下载

（5）单击“完成”按钮，LiveUpdate 窗口关闭，出现“正在更新病毒防护文件”对话框，如图 2-29 所示，提示正在安装下载的升级程序。

2．扫描计算机

查找病毒操作步骤如下。

（1）选择“开始”|“程序”| Symantec Client Security |“Symantec Antivirus 客户端”命令，出现如图 2-25 所示。

（2）选择左边窗口中的“Symantec Antivirus 企业版”|“扫描”|“扫描计算机”命令，右边窗口中提示选择需要扫描的项，单击即可。如图 2-30 所示。

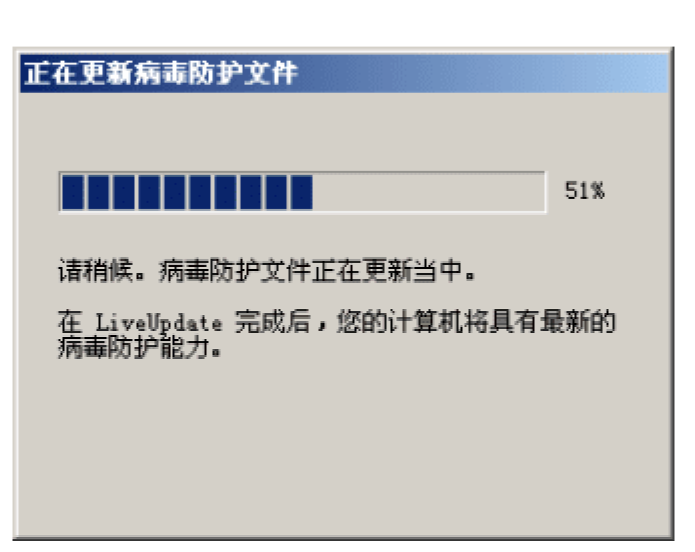
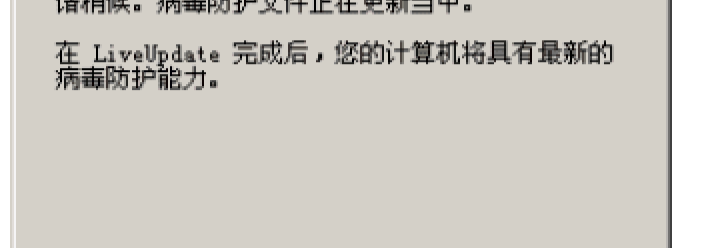



图 2-29　正在更新病毒防护文件提示

图 2-30　选择扫描项目窗口

（3）完成选择以后，单击窗口右下角的“扫描”按钮，系统开始对指定范围的文件进行扫描，如图 2-31 所示。

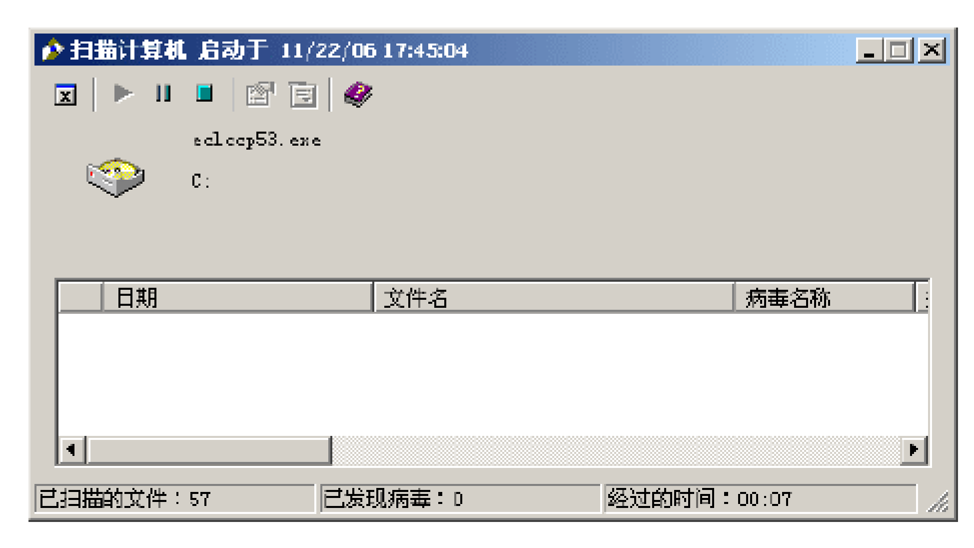


图 2-31　扫描计算机窗口

> **提示：** 杀毒软件发现病毒后通常会直接杀毒，如果不能杀掉，就会对感染病毒的文件进行隔离或者要求删除文件，防止其感染其他的文件。当提示是否删除被感染的病毒文件时，需要考虑被感染病毒文件是否是系统文件或者有用的数据文件。如果是的话，就不能删除文件，否则会造成系统无法启动或者数据丢失，此时应该根据文件中内容的重要性，先作处理，比如将内容复制出来，然后再删除文件，对于隔离的文件可以在适当的时候再恢复，即可对其中的内容进行备份，所以杀毒软件通常情况下会优先选择隔离文件。

（4）在扫描过程中，杀毒程序会自动对发现的病毒进行清除。杀毒过程需要的时间长度与文件数量的多少有关。

3．杀毒软件配置

杀毒软件配置操作步骤如下。

（1）选择“开始”|“程序”| Symantec Client Security |“Symantec Antivirus 客户端”命令，出现如图 2-25 所示。

（2）选择左边窗口中的“Symantec Antivirus 企业版”|“配置”|“文件系统 实时防护”命令，出现配置窗口，如图 2-32 所示。

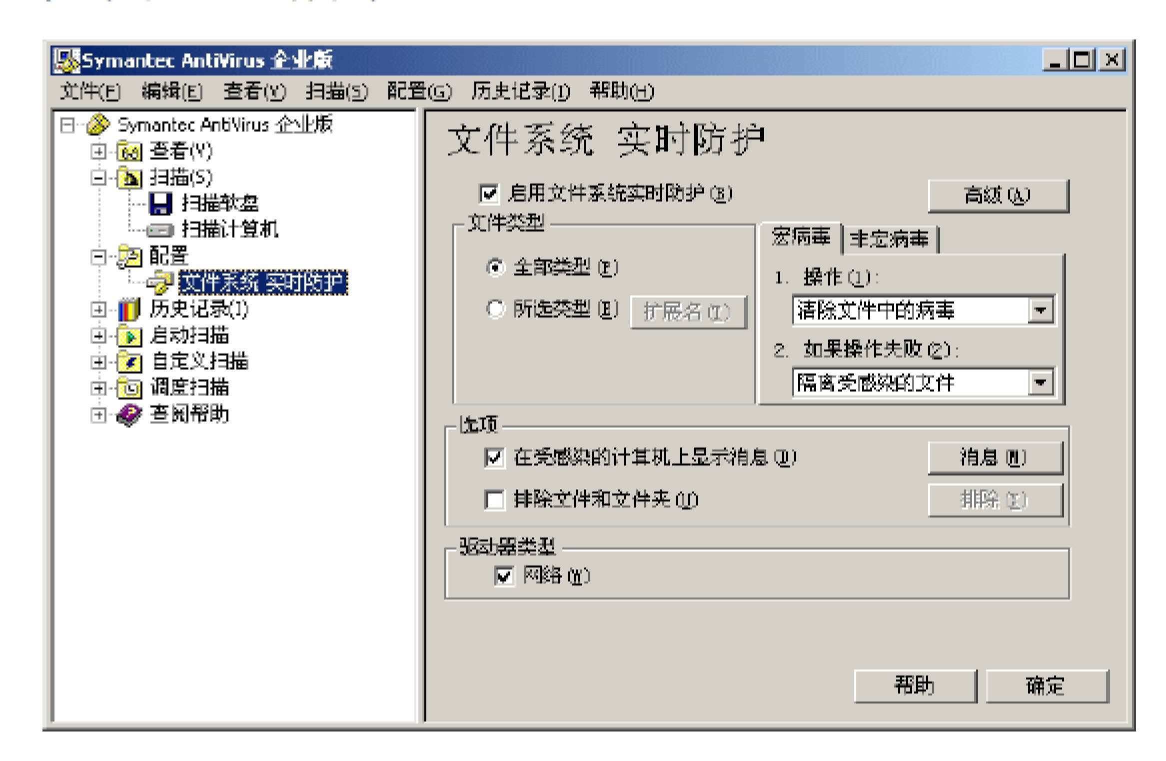


图 2-32　配置窗口

（3）选择“启用文件系统实时防护”复选框，表示杀毒软件会实时扫描当前操作的文件，判断其中是否存在病毒，这项功能对保护计算机免受病毒攻击具有重要作用，比如当从网上下载文件时，如果下载的文件中包含病毒，系统就会给出提示，同时对该文件进行处理，防止其中的病毒感染整个系统。

（4）在“文件类型”组合框中，选择“全部类型”单选框，这样对系统中所有的文件操作都进行扫描，从而防止病毒入侵系统，也可以根据特殊的需要，只扫描指定的文件类型（根据扩展名来定）。

（5）选择“宏病毒”选项卡，在“操作”下拉列表中有 4 个选项，选择“清除文件中的病毒”，这是效果最好的选择，病毒被清除，文件不受影响，在“如果操作失败”下拉列表中有 3 个选项，选择“隔离受感染的文件”，这样即使病毒清除病毒时失败，系统也会将被病毒感染的文件隔离开来，防止其感染其他文件。

（6）选择“非宏病毒”选项卡，将其设置为和宏病毒的设置一样就可以了。

（7）在“选项”组合框中选择“在受感染的计算机上显示消息”，然后单击“消息”按钮，出现如图 2-33 所示。

（8）在“显示消息”对话框中可以设置，当发现计算机病毒时，需要显示与计算机相关的哪些信息，以便对计算机病毒进行处理。需要了解这里设置的具体意义，可以单击“帮助”按钮，出现如图 2-34 所示。

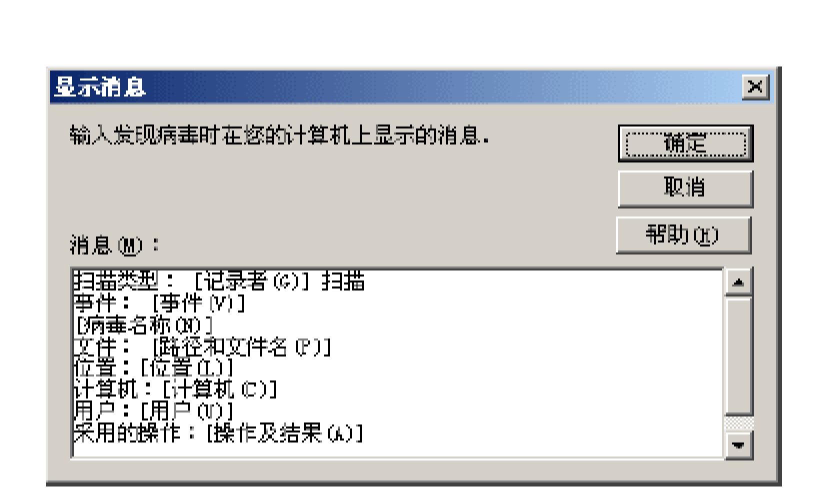


图 2-33　病毒提示消息格式设置

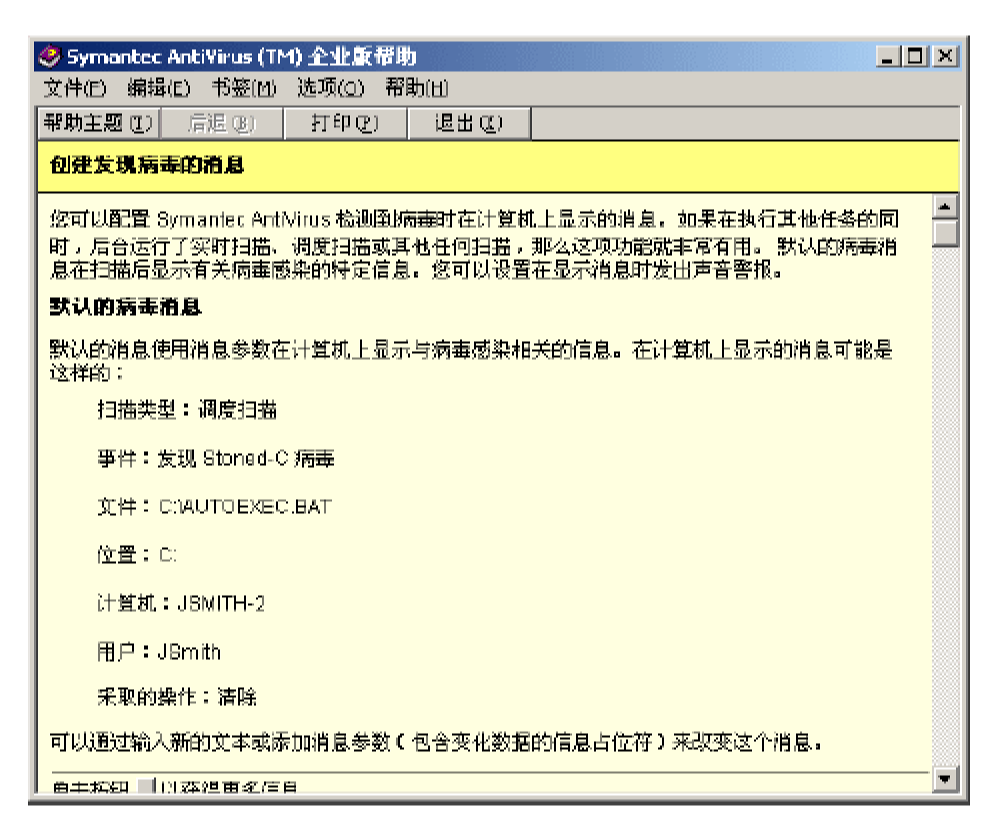


图 2-34　帮助窗口

（9）通过帮助系统提供的帮助信息，可以设置成在发现计算机病毒时需要得到的信息。设置完成后，单击“确定”按钮，让设置生效。

（10）在“选项”组合框中，选择“排除文件和文件夹”，单击“排除”按钮，可以设置不需要扫描的文件类型和文件夹，通常不进行这样的设置，因为计算机病毒种类繁多，感染和传播的方式各异，如果对某些类型的文件或者文件夹不扫描，那么很可能病毒就会隐藏在这些地方。

（11）在“驱动器类型”组合框中，选择“网络”复选框，这样当计算机访问其他计算机上的文件时，也对文件进行扫描，如果发现病毒也像本地计算机一样进行处理，这样可以确保在访问其他计算机时避免被病毒感染。

（12）单击“高级”按钮，出现“文件系统高级选项”对话框，可以根据需要设置灵活的选择，如图 2-35 所示。

（13）选择“受到访问或更改（创建、打开、移动、复制或运行时扫描）”单选框，确保文件在有可能被病毒感染的情况下进行扫描，以最大程度地发现病毒。

（14）在“自动启用”组合框中，选择“实时防护被禁用”复选框，然后设置一个时间间隔来重新启动实时防护，这样确保实时防护不会因为被禁用以后忘记启用而造成病毒的入侵。

（15）在“备份选项”组合框中，选择“尝试修复前备份文件”复选框，这样当文件因修复而损坏时，还可以用其备份文件，有效提高了文件的安全性。

（16）在“其他高级选项”组合框中，单击“启发式”按钮，出现“启发式扫描选项”对话框，如图 2-36 所示，设置完成单击“确定”按钮返回。

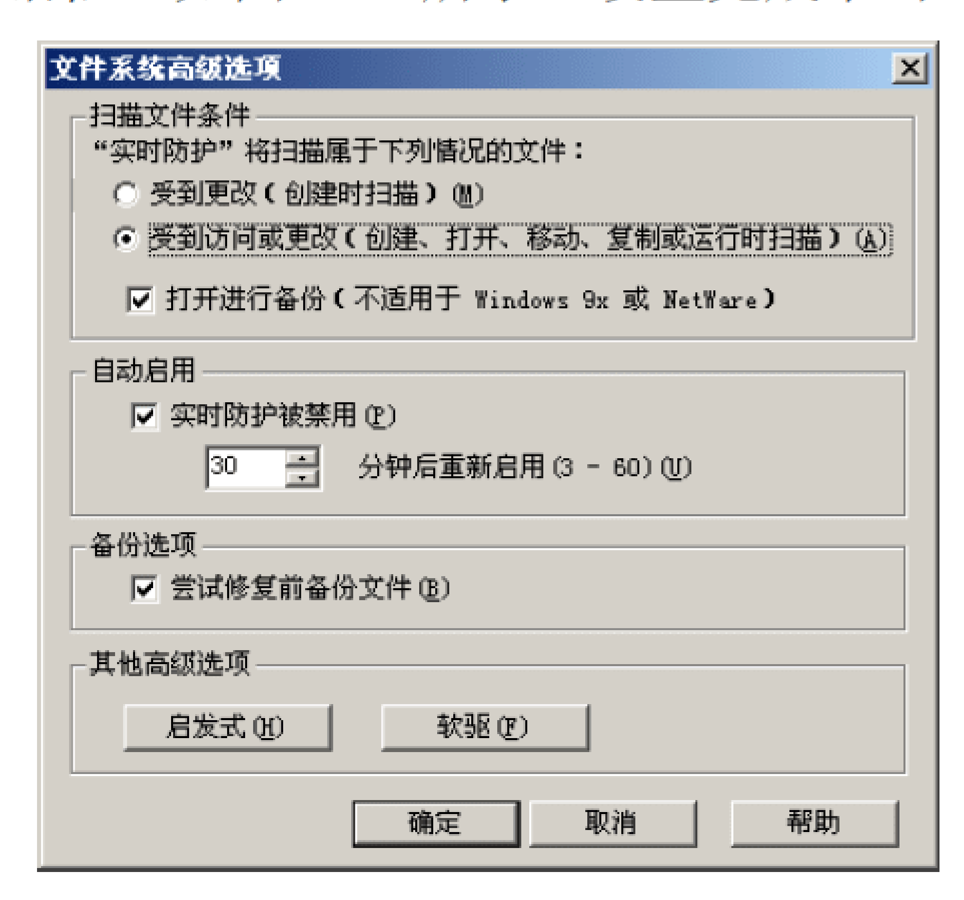




图 2-35 文件系统高级选项



图 2-36 启发式扫描选项设置

（17）单击“软驱”按钮，出现“检查软盘”对话框，如图 2-37 所示，选择默认设置，单击“确定”按钮返回。

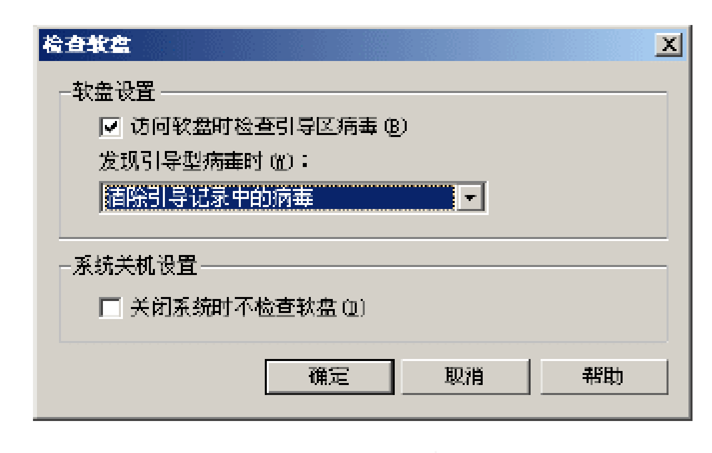


图 2-37 软盘设置

（18）在“文件系统高级选项”对话框中，单击“确定”按钮，完成对应设置。

（19）在配置窗口中，单击“确定”按钮，让刚才进行的所有设置生效。

习题

1．简述计算机病毒的特点。

2．计算机病毒有哪些危害？

3．计算机病毒预防包括哪些内容？

4．选择一种杀毒软件来安装并完成对计算机上的文件进行扫描。

5．在 Windows 进程查看中查看计算机的运行情况，并判断是否有异常。

第3章 数据加密

教学提示

从本质上看，网络安全就是网络上的信息安全。信息安全技术主要包括监控、扫描、检测、加密、认证、防攻击、防病毒以及审计等几个方面，其中加密技术是信息安全的核心技术，已经渗透到大部分安全产品之中，并正向芯片化方向发展。

计算机加密技术是网络信息安全技术的核心技术之一，对其进行深入研究，充分发挥其在网络信息安全中的作用具有重要意义，尤其是在网络信息安全面临“内忧外患”的严峻形势下更是如此。本章将对计算机加密技术的相关知识进行讲解，内容包括加密技术的基本概念、常见的加密算法以及加密技术的应用等内容。

通过对本章的学习，对数据加密技术的发展、基本概念、加密算法以及应用有较深入的理解，特别是对称加密算法和公开密钥加密算法的理解。在实际的网络安全规划、实施过程中充分考虑加密技术的合理、有效利用，提高网络系统的安全性。

教学重点

- 加密技术的基本概念。
- 对称加密算法的理解。
- 公开密钥算法的理解。
- 加密技术的应用。

3.1 数据加密概述

目前企业面临的计算环境和过去有很大的变化，许多数据资源能够依靠网络来远程存取，而且越来越多的通信依赖于公共网络（如 Internet），而这些环境并不保证实体间的安全通信，数据在传输过程中可能被其他人读取或篡改。

加密将防止数据被查看或修改，并在原本不安全的信道上提供安全的通信信道，它能达到以下目的。

（1）保密性：防止用户的标识或数据被读取。

（2）数据完整性：防止数据被更改。

（3）身份验证：确保数据发自特定的一方。

3.1.1 数据加密

密码是实现秘密通信的主要手段，是隐蔽语言、文字、图像的特种符号。凡是用特种符号按照通信双方约定的方法把电文的原型隐蔽起来，不为第三者所识别的通信方式称为密码通信。在计算机通信中，采用密码技术将信息隐蔽起来，再将隐蔽后的信息传输出去，使信息在传输过程中即使被窃取或截获，窃取者也不能了解信息的内容，从而保证信息传

输的安全。

任何一个加密系统至少包括以下 4 个组成部分：

（1）未加密的报文，也称明文；

（2）加密后的报文，也称密文；

（3）加密解密设备或算法；

（4）解密的密钥。

在保障信息安全各种功能特性的诸多技术中，密码技术是信息安全的核心和关键技术，如图 3-1 所示。通过数据加密技术，可以在一定程度上提高数据传输的安全性，保证传输数据的完整性。在数据加密系统中，密钥控制加密和解密过程，一个加密系统的全部安全性是基于密钥的，而不是基于算法，所以加密系统的密钥管理是一个非常重要的问题。

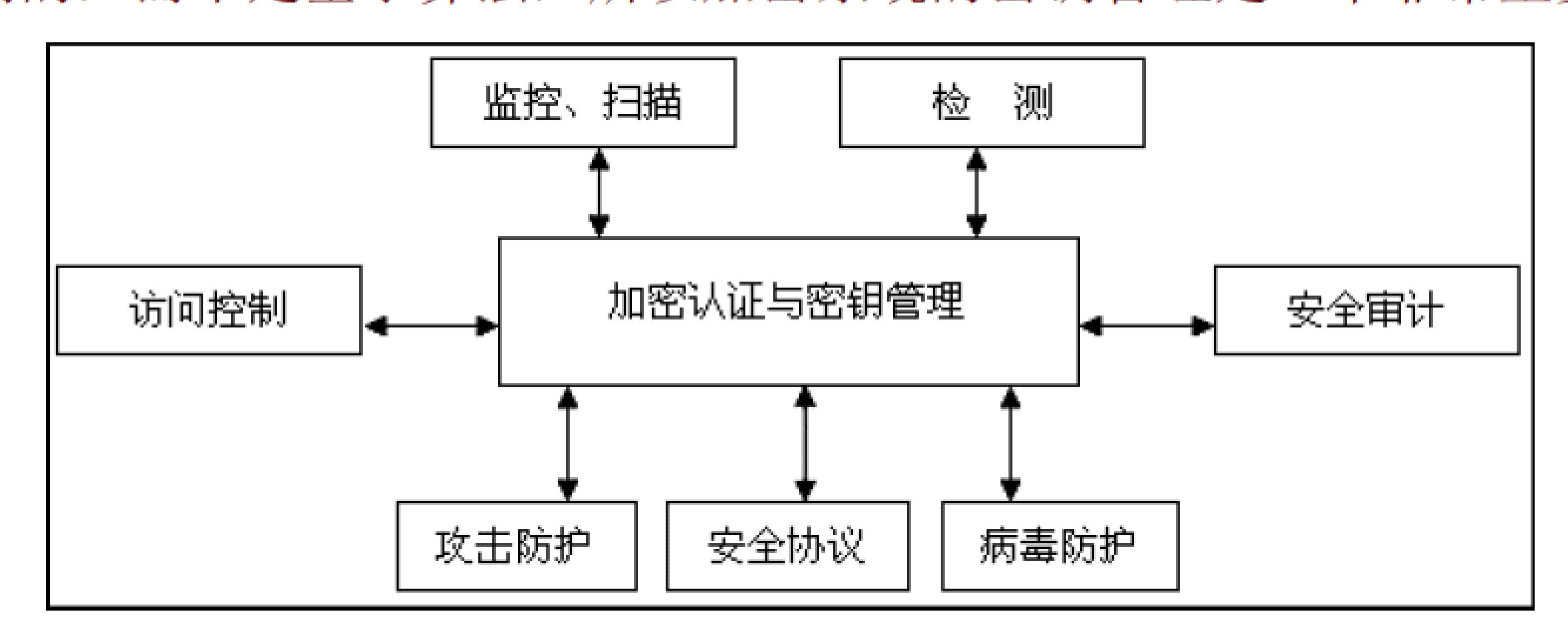


图 3-1　信息安全技术的体系结构图

数据加密过程就是通过加密系统把原始的数字信息（明文），按照加密算法变换成与明文完全不同的数字信息（密文）的过程，如图 3-2 所示。

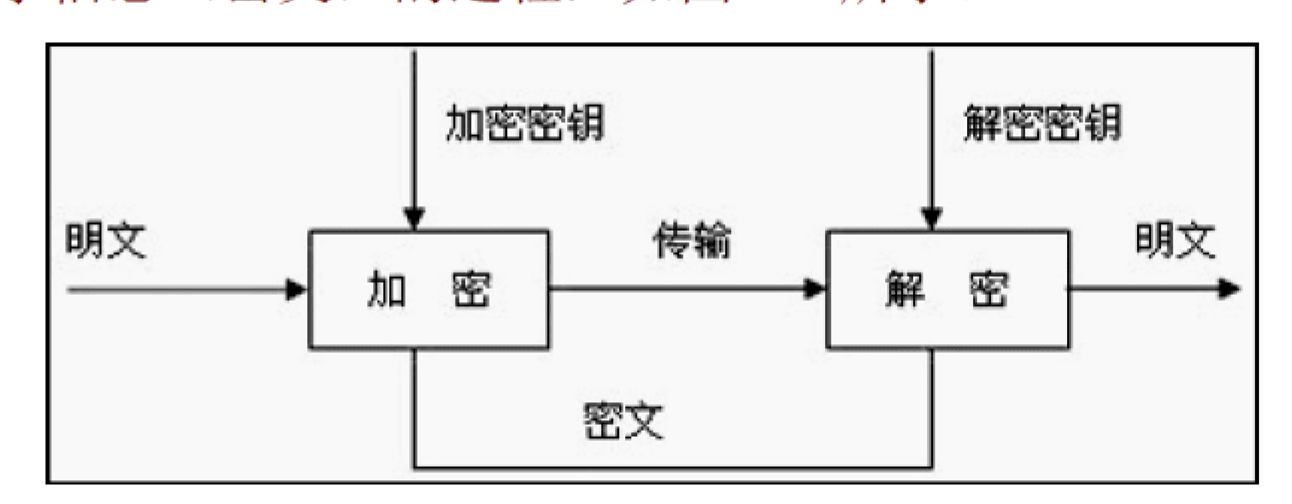


图 3-2　加密解密过程示意图

数据加密技术是为提高信息系统及数据的安全性和保密性，防止秘密数据被外部破解所采用的主要技术手段之一。按照作用的不同，数据加密技术主要分为数据传输、数据存储、数据完整性的鉴别以及密钥管理技术 4 种。

1．数据传输加密技术

数据传输加密技术的目的是对传输中的数据流加密，常用的方法有链路加密、节点加密和端到端加密。

1）链路加密

链路加密是指传输数据仅在物理层前的数据链路层进行加密，不考虑信源和信宿，它用于保护通信节点间的数据，接收方是传送路径上的各台节点机，信息在每台节点机内都要被解密和再加密，依次进行，直至到达目的地。

2）节点加密

与链路加密类似的节点加密方法，是在节点处采用一个与节点机相连的密码装置，密

文在该装置中被解密并被重新加密，明文不通过节点机，避免了链路加密节点处易受攻击的缺点。

3）端到端加密

端到端加密是为数据从一端到另一端提供的加密方式。数据在发送端被加密，在接收端解密，中间节点处不以明文的形式出现。端到端加密是在应用层完成的。

2. 数据存储加密技术

数据存储加密技术的目的是防止在存储环节上的数据失密，可分为密文存储和存取控制两种。前者一般是通过加密算法转换、附加密码、加密模块等方法实现；后者则是对用户资格、权限加以审查和限制，防止非法用户存取数据或合法用户越权存取数据。

3. 数据完整性鉴别技术

数据完整性鉴别技术的目的是对介入信息的传送、存取、处理的人的身份和相关数据内容进行验证，达到保密的要求，一般包括口令、密钥、身份、数据等项的鉴别，系统通过对比验证对象输入的特征值是否符合预先设定的参数，实现对数据的安全保护。

4. 密钥管理技术

为了数据使用的方便，数据加密在许多场合集中表现为密钥的应用，因此密钥往往是保密与窃密的主要对象。密钥的媒体有磁卡、磁带、磁盘、半导体存储器等。密钥的管理技术包括密钥的产生、分配保存、更换与销毁等各环节上的保密措施。

3.1.2 基本概念

数据加密的基本过程就是对原来为明文的文件或数据按某种算法进行处理，使其成为不可读的一段代码，通常称为“密文”，使其只能在输入相应的密钥之后才能显示出本来的内容，通过这样的途径来达到保护数据不被非法人窃取、阅读的目的。该过程的逆过程为解密，即将该编码信息转化为其原来数据的过程。

1. 加密的理由

加密在网络上的作用就是防止有用或私密信息在网络上被拦截和窃取。一个简单的例子就是密码的传输，计算机密码极为重要，许多安全防护体系是基于密码的，密码的泄露在某种意义上来讲意味着其安全体系的全面崩溃。

通过网络进行登录时，所输入的密码以明文的形式被传输到服务器，而网络上的窃听是一件极为容易的事情，所以很有可能黑客会窃取得用户的密码，如果用户是 Root 用户或 Administrator 用户，那后果将是极为严重的。

如果公司在进行着某个招标项目的投标工作，工作人员通过电子邮件的方式把他们单位的标书发给招标单位，如果此时有另一位竞争对手从网络上窃取到标书，从中知道投标的标的，那后果将是怎样，相信不用多说也明白。

这样的例子实在是太多了，解决上述难题的方案就是加密，加密后的口令即使被黑客获得也是不可读的，加密后的标书没有收件人的私钥也就无法解开，标书成为一大堆无任何实际意义的乱码。总之，无论是单位还是个人在某种意义上来说加密也成为当今网络社会进行文件或邮件安全传输的时代象征。

数字签名就是基于加密技术的，它的作用就是用来确定用户是否是真实的。应用最多的还是电子邮件，如当用户收到一封电子邮件时，邮件上面标有发信人的姓名和信箱地址，

很多人可能会简单地认为发信人就是信上说明的那个人，但实际上伪造一封电子邮件对于一个通常人来说是极为容易的事。在这种情况下，就要用到加密技术基础上的数字签名，用它来确认发信人身份的真实性。

类似数字签名技术的还有一种身份认证技术，有些站点提供入站 FTP 和 WWW 服务，当然用户通常接触的这类服务是匿名服务，用户的权力要受到限制，但也有的这类服务不是匿名的，如某公司为了信息交流提供用户的合作伙伴非匿名的 FTP 服务，或开发小组把他们的 Web 网页上载到用户的 WWW 服务器上，现在的问题就是，用户如何确定正在访问用户的服务器的人就是用户认为的那个人，身份认证技术就是一个好的解决方案。

在这里需要强调一点的就是，文件加密不只用于电子邮件或网络上的文件传输，其实也可应用静态的文件保护，以防他人窃取其中的信息。

2．两类加密方法

加密技术通常分为两大类：“对称式”和“非对称式”。

对称式加密就是加密和解密使用同一个密钥，通常称之为 Session Key，这种加密技术目前被广泛采用，如美国政府所采用的 DES 加密标准就是一种典型的“对称式”加密法，它的 Session Key 长度为 56 位。

非对称式加密就是加密和解密所使用的不是同一个密钥，通常有两个密钥，称为“公钥”和“私钥”，它们两个必须配对使用，否则不能打开加密文件。这里的“公钥”是指可以对外公布的，“私钥”则不能，只能由持有人一个人知道。它的优越性就在这里，因为对称式的加密方法如果是在网络上传输加密文件就很难把密钥告诉对方，不管用什么方法都有可能被别人窃听到。而非对称式的加密方法有两个密钥，且其中的“公钥”是可以公开的，也就不怕别人知道，收件人解密时只要用自己的私钥即可，这样就很好地避免了密钥的传输安全性问题。

3．数据摘要算法

摘要是一种防止改动的方法，其中用到的函数叫摘要函数。这些函数的输入可以是任意大小的消息，而输出是一个固定长度的摘要。摘要有这样一个性质，如果改变了输入消息中的任何东西，甚至只有一位，输出的摘要将会发生不可预测的改变，也就是说输入消息的每一位对输出摘要都有影响。总之，摘要算法从给定的文本块中产生一个数字签名，数字签名可以用于防止有人从一个签名上获取文本信息或改变文本信息内容和进行身份认证。

数据摘要算法是密码学算法中非常重要的一个分支，它通过对所有数据提取指纹信息以实现数据签名、数据完整性校验等功能，由于其不可逆性，有时候会被用做敏感信息的加密。数据摘要算法也被称为哈希（Hash）算法或散列算法。常用的数据摘要算法主要有以下几大类。

1）CRC8、CRC16、CRC32

CRC（Cyclic Redundancy Check，循环冗余校验）算法出现时间较长，应用也十分广泛，尤其是通信领域，现在应用最多的就是 CRC32 算法，它产生一个 4 字节（32 位）的校验值，一般是以 8 位十六进制数。CRC 算法的优点在于简便、速度快，严格地来说，CRC 更应该被称为数据校验算法，但其功能与数据摘要算法类似，因此也作为测试的可选算法。

在 WinRAR、WinZIP 等软件中，也是以 CRC32 作为文件校验算法的。一般常见的

简单文件校验（Simple File Verify, SFV）也是以 CRC32 算法为基础，它通过生成一个后缀名为.SFV 的文本文件，这样任何时候都可以将文件内容 CRC32 运算的结果与.SFV 文件中的值对比来确定此文件的完整性。

2）MD2、MD4、MD5

这是应用非常广泛的一个算法家族，尤其是 MD5（Message-Digest Algorithm 5，消息摘要算法版本 5），它由 MD2、MD3、MD4 发展而来，由 Ron Rivest（RSA 公司）在 1992 年提出，目前被广泛应用于数据完整性校验、数据（消息）摘要、数据加密等。MD2、MD4、MD5 都产生 16 字节（128 位）的校验值，一般用 32 位十六进制数表示。MD2 的算法较慢但相对安全，MD4 速度很快，但安全性下降，MD5 比 MD4 更安全、速度更快。

目前在互联网上进行大文件传输时，都要用 MD5 算法产生一个与文件匹配的、存储 MD5 值的文本文件（后缀名为.md5 或.md5sum），这样接收者在接收到文件后，就可以利用与 SFV 类似的方法来检查文件完整性，目前绝大多数大型软件公司或开源组织都是以这种方式来校验数据完整性，而且部分操作系统也使用此算法来对用户密码进行加密，另外，它也是目前计算机犯罪中数据取证的最常用算法。

3）SHA1、SHA256、SHA384、SHA512

SHA（Secure Hash Algorithm，安全哈希算法）是由美国专门制定密码算法的标准机构——美国国家标准技术研究院（NIST）制定的，SHA 系列算法的摘要长度分别为：SHA 为 20 字节（160 位），SHA256 为 32 字节（256 位），SHA384 为 48 字节（384 位），SHA512 为 64 字节（512 位），由于它产生的数据摘要的长度更长，因此更难以发生碰撞，因此也更为安全，它是未来数据摘要算法的发展方向。由于 SHA 系列算法的数据摘要长度较长，因此其运算速度与 MD5 相比，也相对较慢。

目前 SHA1 的应用较为广泛，主要应用于认证授权和数字证书中，另外在目前互联网中流行的 BT 软件中，也是使用 SHA1 来进行文件校验的。

4）RIPEMD、TIGER 等

RIPEMD 是 Hans Dobbertin 等 3 人在对 MD4，MD5 缺陷分析基础上，于 1996 年提出来的，有 4 个标准即 128、160、256 和 320，其对应输出长度分别为 16 字节、20 字节、32 字节和 40 字节。

TIGER 由 Ross 在 1995 年提出。Tiger 号称是最快的 Hash 算法，专门为 64 位机器做了优化。

4．密钥的管理

密钥既然要求保密，这就涉及到密钥的管理问题，管理不好，密钥同样可能被无意识地泄露，并不是有了密钥就高枕无忧，任何保密也只是相对的，是有时效的。要管理好密钥还要注意以下几个方面。

1）密钥的使用要注意时效和次数

如果用户可以一次又一次地使用同样密钥与别人交换信息，那么密钥也同其他任何密码一样存在着一定的安全性，虽然说用户的私钥是不对外公开的，但是也很难保证私钥长期的保密性，很难保证长期以来不被泄露。如果某人偶然地知道了用户的密钥，那么用户曾经和另一个人交换的每一条消息都不再是保密的了。另外使用一个特定密钥加密的信息越多，提供给窃听者的材料也就越多，从某种意义上来讲也就越不安全了。

因此，一般强调仅将一个对话密钥用于一条信息中或一次对话中，或者建立一种按时更换密钥的机制以减小密钥暴露的可能性。

2）多密钥的管理

假设在某机构中有 100 个人，如果他们任意两个人之间可以进行秘密对话，那么总共需要多少密钥呢？每个人需要知道多少密钥呢？也许很容易得出答案，如果任何两个人之间要不同的密钥，则总共需要 4950 个密钥，而且每个人应记住 99 个密钥。如果机构的人数是 1000、10000 个人或更多，这种办法就显然过于愚蠢了，管理密钥将是一件可怕的事情。

有一种较好的解决方案，它是由 MIT 发明的，使保密密钥的管理和分发变得十分容易，但这种方法本身还存在一定的缺点。为能在因特网上提供一个实用的解决方案，Kerberos 建立了一个安全的、可信任的密钥分发中心（Key Distribution Center，KDC），每个用户只要知道一个和 KDC 进行会话的密钥就可以了，而不需要知道成百上千个不同的密钥。

假设用户甲想要和用户乙进行秘密通信，则用户甲先和 KDC 通信，用只有用户甲和 KDC 知道的密钥进行加密，用户甲告诉 KDC 他想和用户乙进行通信，KDC 会为用户甲和用户乙之间的会话随机选择一个对话密钥，并生成一个标签，这个标签由 KDC 和用户乙之间的密钥进行加密，并在用户甲启动和用户乙对话时，用户甲会把这个标签交给用户乙。这个标签的作用是让用户甲确信和他交谈的是用户乙，而不是冒充者。因为这个标签是由只有用户乙和 KDC 知道的密钥进行加密的，所以即使冒充者得到用户甲发出的标签也不可能进行解密，只有用户乙收到后才能够进行解密，从而确定了与用户甲对话的人就是用户乙。

当 KDC 生成标签和随机会话密码，就会把它们用只有用户甲和 KDC 知道的密钥进行加密，然后把标签和会话密钥传给用户甲，加密的结果可以确保只有用户甲能得到这个信息，只有用户甲能利用这个会话密钥和用户乙进行通话。同理，KDC 会把会话密钥用只有 KDC 和用户乙知道的密钥加密，并把会话密钥传给用户乙。

用户甲会启动一个和用户乙的会话，并用得到的会话密钥加密自己和用户乙的会话，还要把 KDC 传给它的标签传给用户乙以确定用户乙的身份，然后用户甲和用户乙之间就可以用会话密钥进行安全的会话了，而且为了保证安全，这个会话密钥是一次性的，这样黑客就更难进行破解了。同时由于密钥是一次性由系统自动产生的，则用户不必记那么多密钥了，方便了人们的通信。

5．数据加密的标准

最早、最著名的保密密钥或对称密钥加密算法 DES（Data Encryption Standard，数据加密标准）是由 IBM 公司在 20 世纪 70 年代发展起来的，并经政府的加密标准筛选后，于 1976 年 11 月被美国政府采用，DES 随后被美国国家标准局和美国国家标准协会（American National Standard Institute，ANSI）承认。

DES 使用 56 位密钥对 64 位的数据块进行加密，并对 64 位的数据块进行 16 轮编码。在每轮编码时，一个 48 位的“每轮”密钥值由 56 位的完整密钥得出来。DES 用软件进行解码需用很长时间，而用硬件解码速度非常快。幸运的是，当时大多数黑客并没有足够的设备制造出这种硬件设备。在 1977 年，人们估计要耗资两千万美元才能建成一个专门的计算机用于 DES 的解密，而且需要 12 个小时的破解才能得到结果。当时 DES 被认为是一种

十分强大的加密方法。

随着计算机硬件的速度越来越快，制造一台这样特殊的机器的花费已经降到了十万美元左右，而用它来保护十亿美元的银行，那显然是不够保险了。另一方面，如果只用它来保护一台普通服务器，那么 DES 确实是一种好的办法，因为黑客绝不会仅仅为入侵一个服务器而花那么多的钱破解 DES 密文。

另一种非常著名的加密算法就是 RSA 了，RSA（Rivest-Shamir-Adleman）算法是基于大数不可能被质因数分解假设的公钥体系。简单地说就是找两个很大的质数，一个对外公开的为“公钥”（Prblic key），另一个不告诉任何人，称为“私钥”（Private key）。这两个密钥是互补的，也就是说用公钥加密的密文可以用私钥解密，反过来也一样。

假设用户甲要寄信给用户乙，他们互相知道对方的公钥。甲就用乙的公钥加密邮件寄出，乙收到后就可以用自己的私钥解密出甲的原文。由于别人不知道乙的私钥，所以即使是甲本人也无法解密那封信，这就解决了信件保密的问题。另一方面，由于每个人都知道乙的公钥，他们都可以给乙发信，那么乙怎么确信是不是甲的来信呢？那就要用到基于加密技术的数字签名了。

甲用自己的私钥将签名内容加密，附加在邮件后，再用乙的公钥将整个邮件加密（注意这里的次序，如果先加密再签名的话，别人可以将签名去掉后签上自己的签名，从而篡改了签名）。这样这份密文被乙收到以后，乙用自己的私钥将邮件解密，得到甲的原文和数字签名，然后用甲的公钥解密签名，这样一来就可以确保两方面的安全了。

3.2 对称加密算法

对称算法就是加密密钥能够从解密密钥中推算出来，反过来也成立。在大多数对称算法中，加密密钥和解密密钥是相同的。对称加密算法也叫秘密密钥算法或单密钥算法，要求发送者和接收者在安全通信之前，商定一个密钥。对称算法的安全性依赖于密钥，泄露密钥就意味着任何人都能对消息进行加密和解密。

对称算法可分为两类：序列密码（流密码）与分组密码。

序列密码一直是作为军方和政府使用的主要密码技术之一，它的主要原理是，通过伪随机序列发生器产生性能优良的伪随机序列，使用该序列加密信息流，逐位加密得到密文序列，所以，序列密码算法的安全强度完全决定于伪随机序列的好坏。伪随机序列发生器是指输入真随机的较短的密钥（种子）通过某种复杂的运算产生大量的伪随机位流。

序列密码算法将明文逐位转换成密文。该算法最简单的应用如图 3-3 所示。密钥流发生器输出一系列比特流：K_1，K_2，K_3，…，K_i。密钥流跟明文比特流 P_1，P_2，P_3，…，P_i，进行异或运算产生密文比特流。

$$C_i=P_i \oplus K_i$$

在解密端，密文流与完全相同的密钥流异或运算恢复出明文流。

$$P_i=C_i \oplus K_i$$

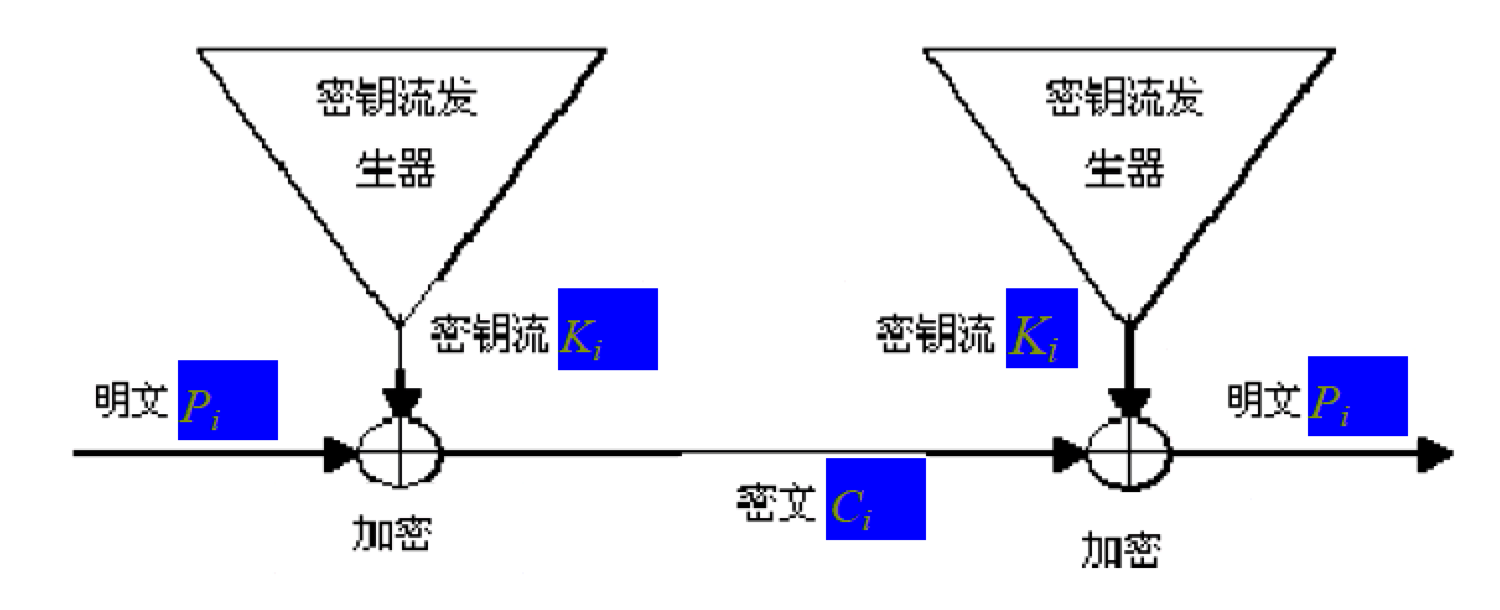


图 3-3　序列密码

对于一个序列如果对所有的 i 总有 $K_{i+p}=K_i$，则序列是以 p 为周期的，满足条件的最小的 p 称为序列的周期。密钥流发生器产生的序列周期应该足够的长，如 250。

基于移位寄存器的序列密码应用十分广泛。一个反馈移位寄存器由两部分组成：移位寄存器和反馈函数。移位寄存器的长度用位表示，如果是 n 位长，称为 n 位移位寄存器。移位寄存器每次向右移动一位，新的最左边的位根据反馈函数计算得到，移位寄存器输出的位是最低位，如图 3-4 所示。

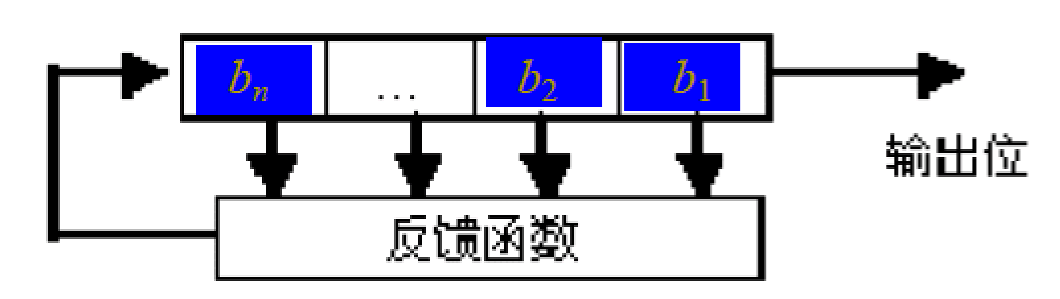


图 3-4　反馈移位寄存器

最简单的反馈移位寄存器是线形反馈移位寄存器，反馈函数是寄存器中某些位简单异或，如图 3-5 所示。

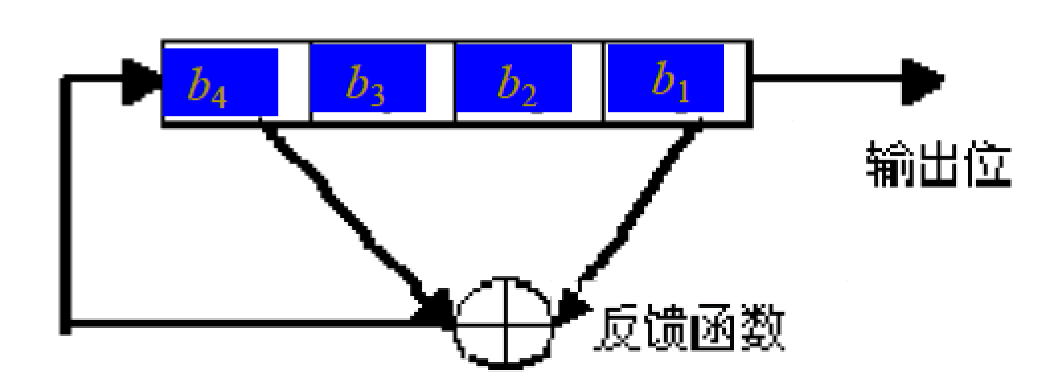


图 3-5　4 位线形反馈移位寄存器

产生好的序列密码的主要途径之一是利用移位寄存器产生伪随机序列，典型方法如下。

（1）反馈移位寄存器：采用非线性反馈函数产生大周期的非线性序列。

（2）利用线性移位寄存器序列加非线性前馈函数，产生前馈序列。

（3）钟控序列，利用一个寄存器序列作为时钟控制另一寄存器序列（或自己控制自己）来产生钟控序列，这种序列具有大的线性复杂度。

分组密码是将明文分成固定长度的组（块），如 64 位一组，用同一密钥和算法对每一块加密，输出也是固定长度的密文。

3.2.1　DES 算法及其基本思想

DES 是 Data Encryption Standard（数据加密标准）的缩写。它是由 IBM 公司研制的一种加密算法，美国国家标准局于 1977 年公布把它作为非机要部门使用的数据加密标准。它主要用于民用敏感信息的加密，后来被国际标准化组织接受作为国际标准。

DES 主要采用替换和移位的方法加密。它用 56 位密钥对 64 位二进制数据块进行加密，

每次加密可对 64 位的输入数据进行 16 轮编码，经一系列替换和移位后，输入的 64 位原始数据转换成完全不同的 64 位输出数据。

DES 算法仅使用最大为 64 位的标准算术和逻辑运算，运算速度快，密钥生产容易，适合于在当前大多数计算机上用软件方法实现，同时也适合于在专用芯片上实现。

DES 算法的弱点是不能提供足够的安全性，因为其密钥容量只有 56 位。由于这个原因，后来又提出了三重 DES 或 3DES 系统，使用 3 个不同的密钥对数据块进行两次或三次加密，该方法比进行普通加密的三次快。其强度大约和 112 位的密钥强度相当。

1．算法框架

DES 对 64 位的明文分组 M 进行操作，M 经过一个初始置换 IP 置换成 m_0，将 m_0 明文分成左半部分和右半部分 $m_0=(L_0，R_0)$，各 32 位长。然后进行 16 轮完全相同的运算，这些运算被称为函数 f，在运算过程中数据与密钥结合。经过 16 轮后，左、右半部分合在一起经过一个末置换，这样就完成了。

在每一轮中，密钥位移位，然后再从密钥的 56 位中选出 48 位。通过一个扩展置换将数据的右半部分扩展成 48 位，并通过一个异或操作替代成新的 32 位数据，在将其置换一次。这 4 步运算构成了函数 f。然后，通过另一个异或运算，函数 f 的输出与左半部分结合，其结果成为新的右半部分，原来的右半部分成为新的左半部分。将该操作重复 16 次，就实现了，如图 3-6 所示。

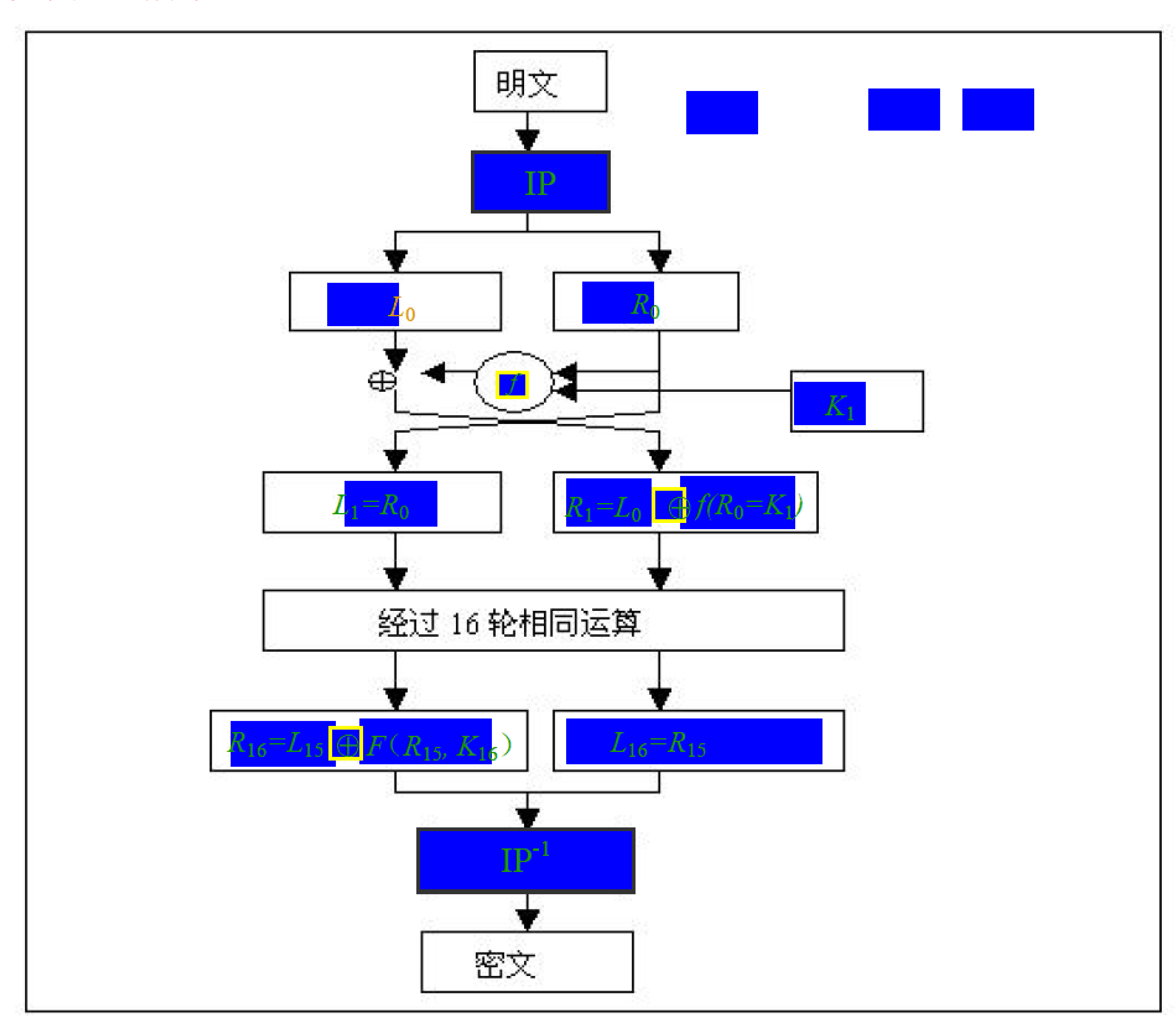


图 3-6　DES 算法框图

2．DES 解密

在经过所有的代替、置换、异或盒循环之后，你也许认为解密算法与加密算法完全不

同。恰恰相反，经过精心选择的各种操作，获得了一个非常有用的性质：加密和解密使用相同的算法。

DES 加密和解密唯一的不同是密钥的次序相反。如果各轮加密密钥分别是 K_1，K_2，K_3，…，K_{16}，那么解密密钥就是 K_{16}，K_{15}，K_{14}，…，K_1。

3.2.2　DES 算法的安全性分析

在 DES 的加密过程中，之所以选择 16 次函数 f 的运算，是因为对低于 16 轮的任意 DES 的已知明文攻击要比穷举攻击更为有效，而当运算次数恰好有 16 轮的时候，只有穷举攻击最有效，所以在分析数据加密标准的安全性时可以用穷举法攻击为例来分析。所谓穷举法，就是已知密文 C 和它对应的明文 P，用一切可能的密钥加密 P，直到 $E(P，K)=C$。这时所用的密钥 K 即为攻击者所要破译的密码。

虽然 DES 密钥的长度为 64 位，但为了确保密钥不发生错误，每个字节的第 8 位实际上是作为奇偶校验的，所以实际起作用的只有 56 位，故在知道明文和密文的情况下只要用穷举法 256 次就能算出密码，这在过去是很难做到的，即使能用上万台小型机来进行运算并破译出来，结果也是得不偿失，但是现在的计算条件则完全可以用可接受的代价算出 DES 密码来。况且在弱密钥等极端情况下，DES 安全性将会受到更大的影响。所以提高 DES 的安全性成为越来越迫切的问题。为此，我们在设计时可以尝试几种经过变形的 DES 算法。

（1）独立子密钥法

如果我们在 DES 的加密过程中使用独立的子密钥，而不是由单一 64 位密钥产生的互相联系的子密钥，由于 16 轮的运算每轮都需要 48 位密钥，这就意味着这种变形后的 DES 算法的密钥长度将变成为 768 位。如果用穷举法来攻击，这个攻击的复杂性将达到 2^{769}，但是这种变形后的算法对差分分析相当敏感，可以只用 263 个选择明文破译，所以这种方法并不能使 DES 算法变得更安全。

（2）增加密钥长度法

为了增加 DES 的安全性，我们可以选择一种增加 DES 密钥长度的方法，实现这种方法最简单最有效的途径就是多重 DES 算法。

现在最常用的多重 DES 算法就是 128 位的 3DES 算法，这也是被 EMV 标准唯一采用的对称密钥算法。3DES 算法是用两个 64 位的密钥对一个明文进行三次加密，整个加密过程就是先用第一个密钥对明文加密， 再用第二个密钥进行解密，然后再用第一个密钥进行加密。解密的时候先用第一个密钥解密，再用第二个密钥加密，最后用第一个密钥解密，用公式表示就是：

$$C=E（D（E（P，K_1），K_2），K_1）$$
$$P=D（E（D（C，K_1），K_2），K_1）$$

这种工作模式我们也称之为加密—解密—加密模式，即 EDE 模式，它不会受到前面间相遇攻击的影响，用穷举法破解它将达到 2^{112}，这在现阶段是非常困难的，所以它在现阶段具有比较高的安全性。

3.2.3 DES 加密算法举例

在此以“世优文件保镖 V1.0”为例说明 DES 加密算法的应用，首先从网上下载安装程序，安装到本地计算机上，因为本软件是一个免费软件，所以可以从各个大的下载网站进行免费下载。

具体的操作步骤如下。

（1）选择“开始”|“程序”|“世优文件保镖 V1.0”命令，出现登录密码输入窗口，如图 3-7 所示。

（2）如果是第一次使用该程序，输入默认密码 4usoft，单击“登录”按钮，出现主窗口，如图 3-8 所示。



图 3-7 登录密码窗口

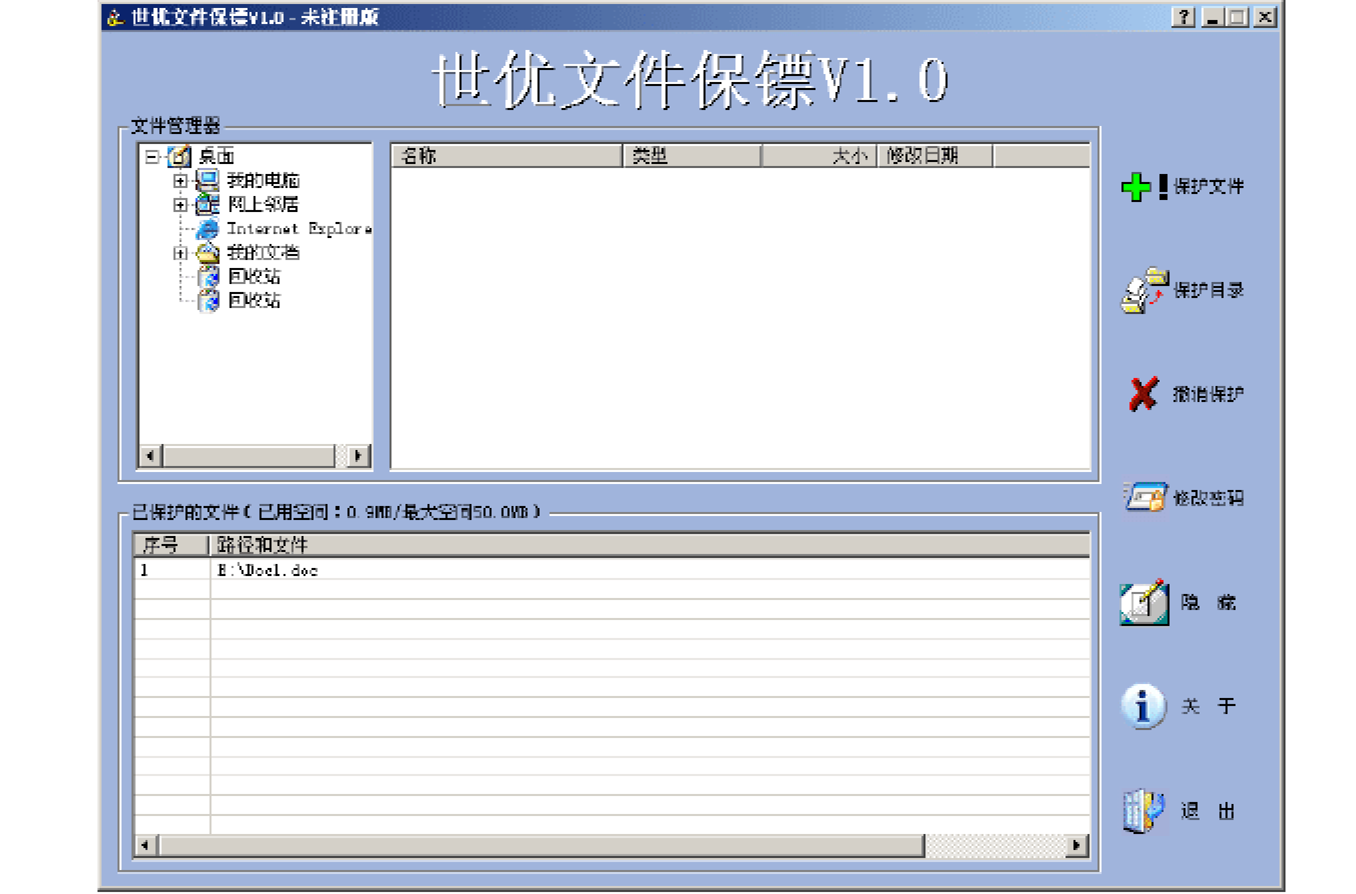


图 3-8 文件保镖主窗口

（3）从“文件管理器”中选择需要进行保护的文件，直接拖放到“已保护文件”列表中即可，找到需要加密的文件，比如 E 盘下的 Doc1.doc 文件，如图 3-9 所示。



图 3-9 被加密的文件 Doc1.doc

（4）将 E 盘根目录下的 Doc1.doc 文件添加到“已保护文件”列表中，此时用 Word 打开 Doc1.doc 文档，可以看到文档的内容，如图 3-10 所示。

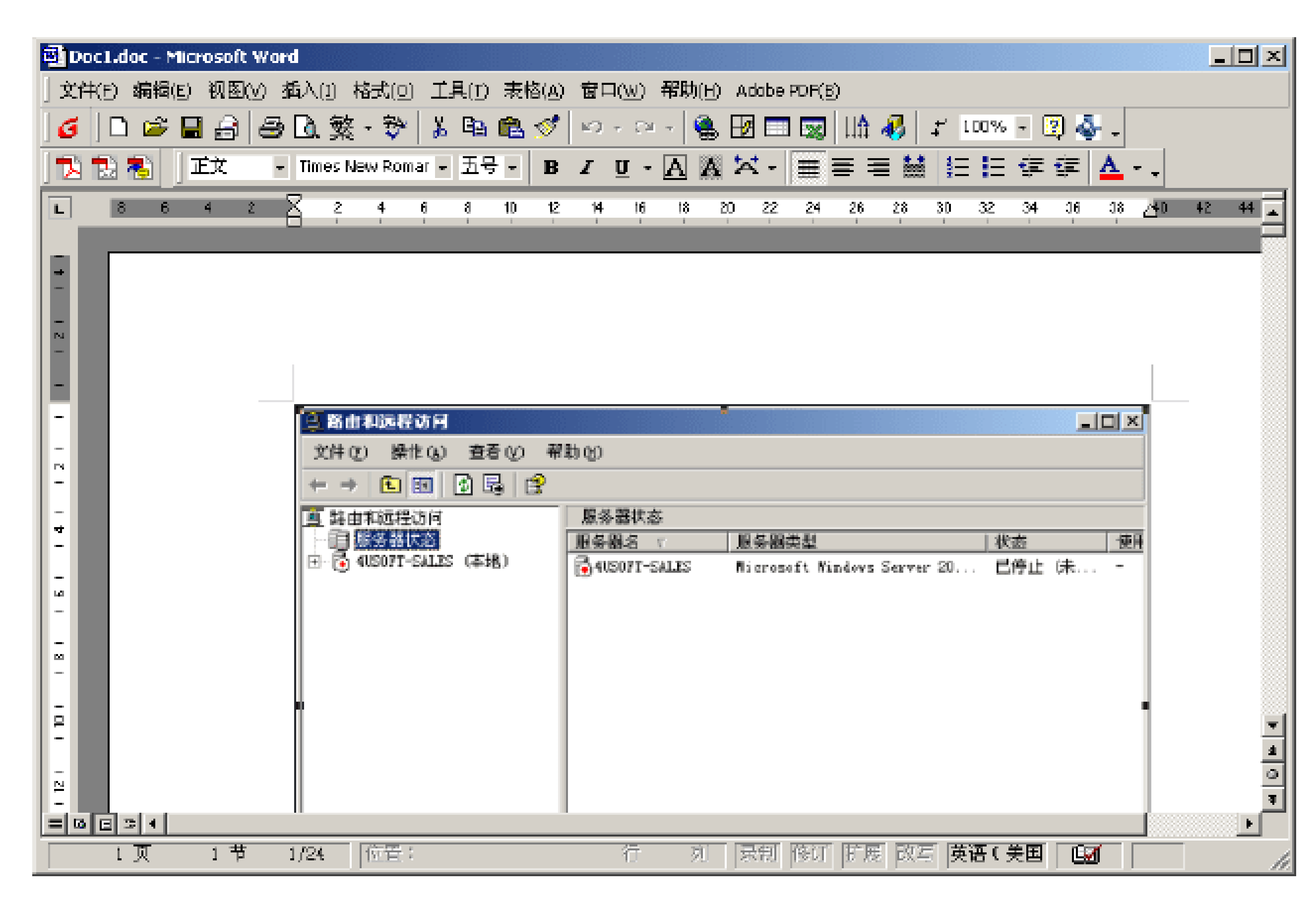
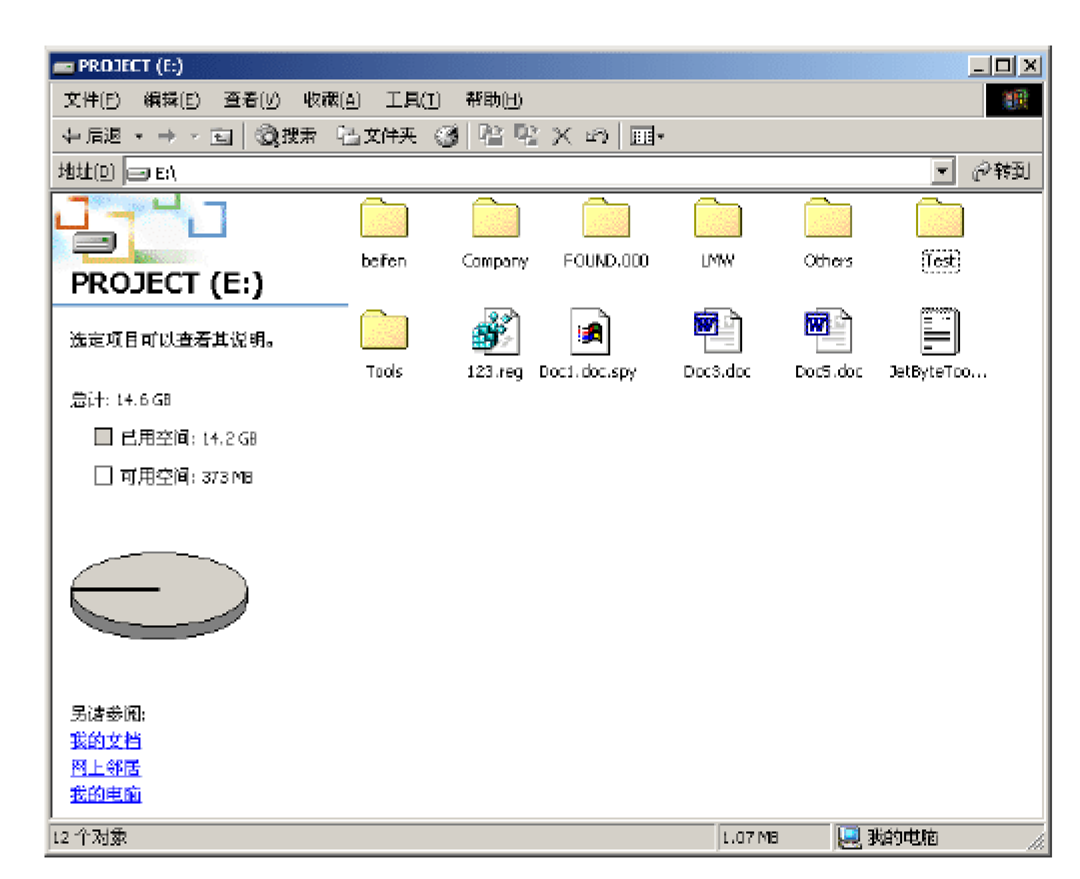


图 3-10　未被加密前的文件内容

（5）然后关闭“世优文件保镖”窗口，可以看到文件的扩展名被改变成 Doc1.doc.spy，图标也被改变了，如图 3-11 所示。

（6）对加密后的文件用 Word 打开，可以看到文档内容如图 3-12 所示，文件的内容已经被加密处理，无法直接通过 Word 对文件内容进行查看，这样就起到保护文档内容的目的了。



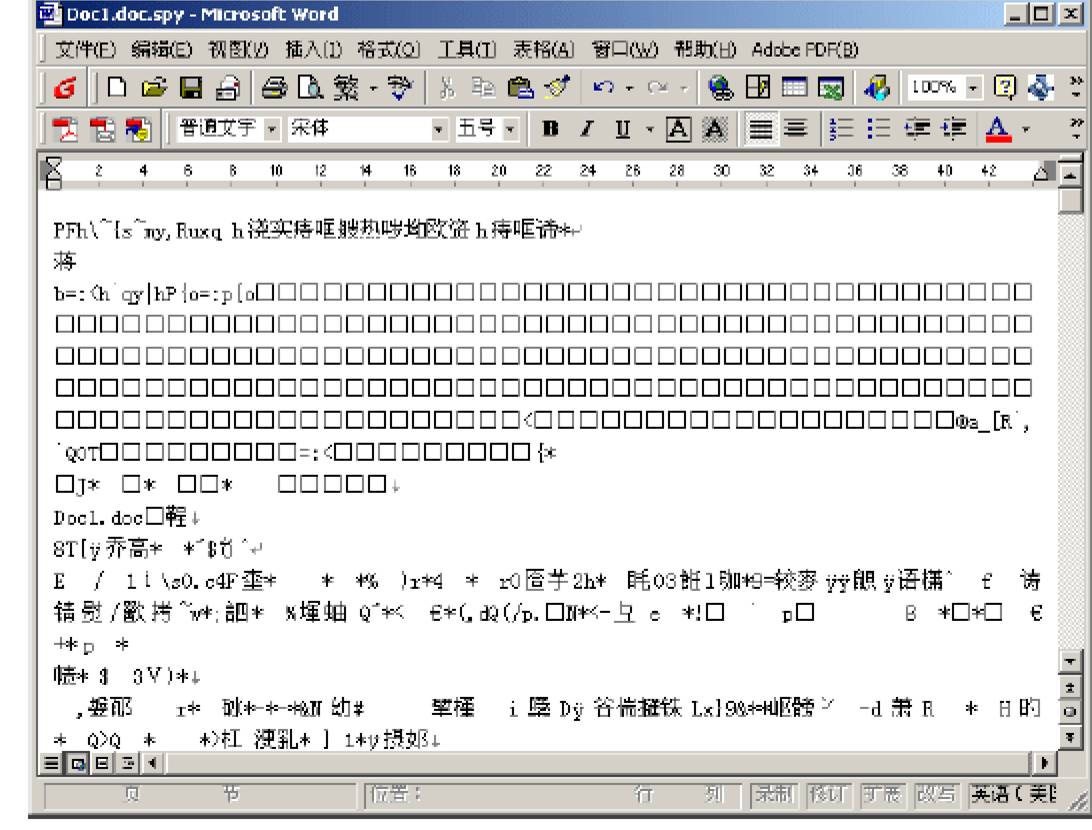


图 3-11　加密后的文件　　　　图 3-12　被加密后的 Word 文档内容

（7）重新启动“世优文件保镖”程序，此时 Doc1.doc.spy 文件消失了，出现 Doc1.doc 文件，然后再打开文件 Doc1.doc，可以看到稳定的内容如图 3-13 所示。

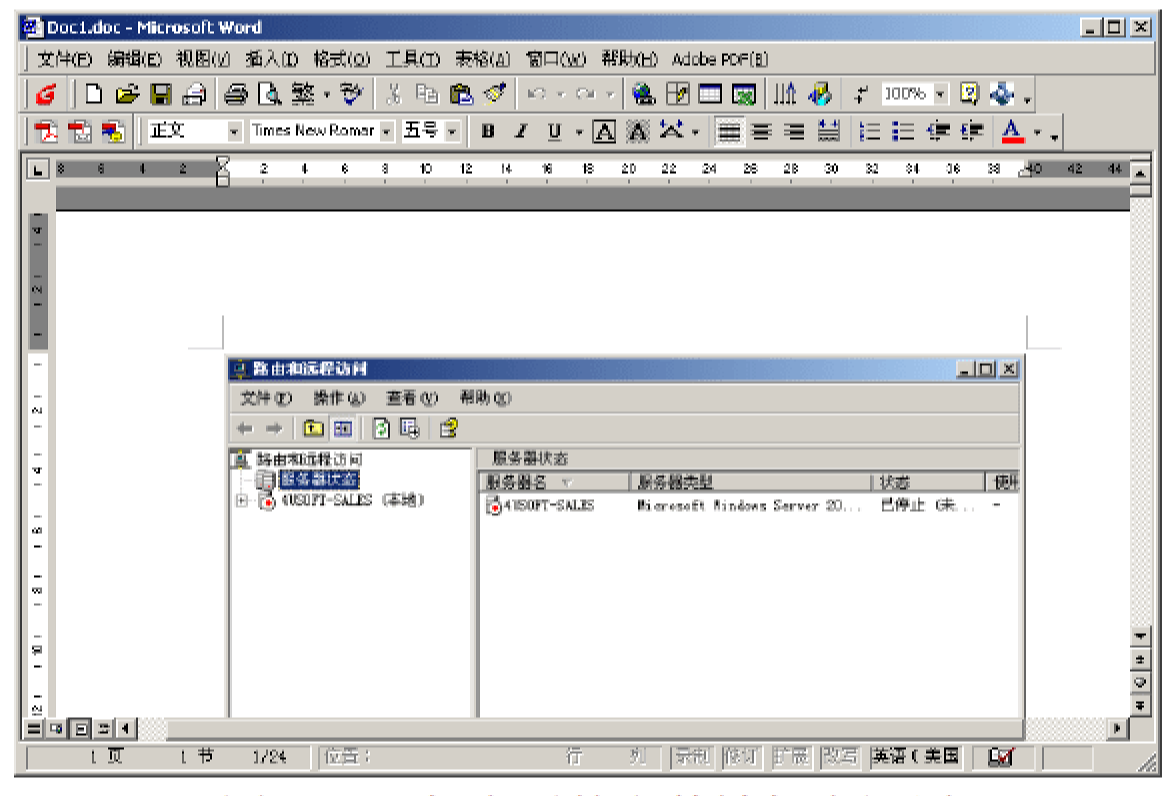


图 3-13　加密后的文件被加密还原

（8）通过上述的过程即可看出，只有在运行“世优文件保镖”程序时才能看到文件的内容（可以通过密码来控制），从而达到加密保护文件的目的。

提示：需要特别注意的是设置的密码需要保存到安全的地方，一方面不能随意让他人知道，另一方面需要自己能够牢记，一旦密码丢失，加密的文件也无法恢复了。

3.3　公开密钥算法

公开密钥算法中用作加密的密钥不同于用作解密的密钥，而且解密密钥不能根据加密密钥计算出来（至少在合理假定的长时间内），所以加密密钥能够公开，每个人都能用加密密钥加密信息，但只有解密密钥的拥有者才能解密信息。在公开密钥算法系统中，加密密钥叫做公开密钥（简称公钥），解密密钥叫做秘密密钥（私有密钥，简称私钥）。

公开密钥算法主要用于加密/解密、数字签名、密钥交换。自从 1976 年公钥密码的思想提出以来，国际上已经出现了许多种公钥密码体制，比较流行的有基于大整数因子分解问题的 RSA 体制和 Rabin 体制、基于有限域上的离散对数问题的 Differ-Hellman 公钥体制和 ElGamal 体制、基于椭圆曲线上的离散对数问题的 Differ-Hellman 公钥体制和 ElGamal 体制。这些密码体制有的只适合于密钥交换，有的只适合于加密/解密。

3.3.1　RSA 算法及其基本思想

RSA（Rivest-Shamir-Adleman）适用于数字签名和密钥交换。RSA 加密算法是目前应用最广泛的公钥加密算法，特别适用于通过 Internet 传送的数据。这种算法以它的三位发明者的名字命名：Ron Rivest、Adi Shamir 和 Leonard Adleman。

RSA 算法的安全性基于分解大数字时的困难（就计算机处理能力和处理时间而言）。在常用的公钥算法中，RSA 与众不同，它能够进行数字签名和密钥交换运算。

RSA 算法既能用于数据加密，也能用于数字签名，RSA 的理论依据为：寻找两个大素数比较简单，而将它们的乘积分解开则异常困难。在 RSA 算法中，包含两个密钥，加密密钥和解密密钥，加密密钥是公开的。

RSA 算法的优点是密钥空间大，缺点是加密速度慢，如果 RSA 和 DES 结合使用，则正好弥补 RSA 的缺点。即 DES 用于明文加密，RSA 用于 DES 密钥的加密。由于 DES 加密速度快，适合加密较长的报文，而 RSA 可解决 DES 密钥分配的问题。

1．RSA 算法

首先，找出三个数，p、q、r。

其中 p、q 是两个相异的质数，r 是与 $(p-1)(q-1)$ 互质的数，

p、q、r 这三个数便是私钥。

接着，找出 m，使得 $rm = 1 \bmod (p-1)(q-1)$，

这个 m 一定存在，因为 r 与 $(p-1)(q-1)$ 互质，用辗转相除法就可以得到了。

再来，计算 $n = pq$，

m、n 这两个数便是公钥。

编码过程是，若参数为 a，将其看成是一个大整数，假设 $a < n$，

如果 $a \geqslant n$ 的话，就将 a 表示成 s 进位（$s \leqslant n$，通常取 $s = 2$^t），

则每一位数均小于 n，然后分段编码。

接下来，计算 $b = a$^$m \bmod n$，（$0 \leqslant b < n$），

b 就是编码后的参数。

解码的过程是，计算 $c = b$^$r \bmod pq$ $(0 \leqslant c < pq)$，

于是，解码完毕。

如果第三者进行窃听时，他会得到几个数：m、n（$=pq$）、b，

他如果要解码的话，必须想办法得到 r，

所以，他必须先对 n 作质因数分解。

要防止他分解，最有效的方法是找两个非常大的质数 p、q，

使第三者作因数分解时发生困难。

2．RSA 的速度

由于进行的都是大量数据的计算，使得 RSA 最快的情况也比 DES 慢上 10 倍，无论是软件还是硬件实现，速度一直是 RSA 的缺陷。一般来说只用于少量数据加密。

3.3.2　RSA 算法的安全性分析

RSA 算法是第一个能同时用于加密和数字签名的算法，也易于理解和操作。RSA 是被研究得最广泛的公钥算法，从提出到现在已近 20 年，经历了各种攻击的考验，逐渐为人们接受，普遍认为是目前最优秀的公钥方案之一。

1．RSA 的安全性

RSA 的安全性依赖于大数分解，但是否等同于大数分解一直未能得到理论上的证明，因为没有证明破解 RSA 就一定需要作大数分解。假设存在一种无须分解大数的算法，那它肯定可以修改成为大数分解算法。目前，RSA 的一些变种算法已被证明等价于大数分解。不管怎样，分解 n 是最显然的攻击方法。现在，人们已能分解多个十进制位的大素数。因此，模数 n 必须选大一些，因具体适用情况而定。

RSA 的主要缺点如下。

（1）产生密钥很麻烦，受到素数产生技术的限制，因而难以做到一次一密。

（2）分组长度太大，为保证安全性，n 至少也要 600 位以上，使运算代价很高，尤其是速度较慢，较对称密码算法慢几个数量级；且随着大数分解技术的发展，这个长度还在增加，不利于数据格式的标准化。

2．RSA 的选择密文攻击

RSA 在选择密文攻击面前很脆弱。一般攻击者是将某一信息作一下伪装，让拥有私钥的实体签署。然后，经过计算就可得到它所想要的信息。实际上，攻击利用的都是同一个弱点，即存在这样一个事实：乘幂保留了输入的乘法结构：

$$(XM)\text{^}d = X\text{^}d * M\text{^}d \bmod n$$

前面已经提到，这个固有的问题来自于公钥密码系统的最有用的特征——每个人都能使用公钥。但从算法上无法解决这一问题，主要措施有两条：一条是采用好的公钥协议，保证工作过程中不对其他实体任意产生信息解密，不对自己一无所知的信息签名；另一条是决不对陌生人送来的随机文档签名，签名时首先使用哈希函数对文档作哈希处理，或同

时使用不同的签名算法。

3．RSA 的公共模数攻击

若系统中共有一个模数，只是不同的人拥有不同的 e 和 d，系统将是危险的。最普遍的情况是同一信息用不同的公钥加密，这些公钥共模而且互质，那么该信息无需私钥就可得到恢复。设 P 为信息明文，两个加密密钥为 e_1 和 e_2，公共模数是 n，则：

$$C_1 = P\hat{}e_1 \bmod n$$

$$C_2 = P\hat{}e_2 \bmod n$$

密码分析者知道 n、e_1、e_2、C_1 和 C_2，就能得到 P。

因为 e_1 和 e_2 互质，故用 Euclidean 算法能找到 r 和 s，满足：

$$r * e_1 + s * e_2 = 1$$

假设 r 为负数，需再用 Euclidean 算法计算 $C_1\hat{}(-1)$，则

$$(C_1\hat{}(-1))\hat{}(-r) * C_2\hat{}s = P \bmod n$$

另外，还有其他几种利用公共模数攻击的方法。总之，如果知道给定模数的一对 e 和 d，一是有利于攻击者分解模数，一是有利于攻击者计算出其他成对的 e 和 d，而无需分解模数。解决办法只有一个，那就是不要共享模数 n。

RSA 的小指数攻击。有一种提高 RSA 速度的建议是使公钥 e 取较小的值，这样会使加密变得易于实现，速度有所提高。但这样做是不安全的，对付办法就是 e 和 d 都取较大的值。

3.3.3 RSA 加密算法举例

在前两节中介绍了对称加密算法 RSA 的基本知识，这里使用对称加密算法来实现数据加密和解密，使用的工具名称为 Swriter，具体的操作过程如下。

提示：Swriter.exe 程序可以从网站上免费下载。

1．建立系统密钥

使用 Swriter 的第一步是建立系统密钥，将自己的加密基数和公钥发送给要与之通信的人，并将其他人的加密基数和公钥输入到自己的系统中，下面是具体的操作步骤。

（1）当第一次运行 Swriter.exe 程序时，出现如图 3-14 所示的界面，会提示建立系统密钥，建立系统密钥以后就不会出现该提示了。



图 3-14　建立系统密钥提示

（2）需要使用该工具进行加密的第一部就是需要建立系统密钥，所以单击“是”按钮，出现建立系统密钥窗口，如图 3-15 所示。

（3）在“生成/改变密钥”对话框的文本框中输入任意文本信息，然后单击“确定”按钮，出现“公开密钥”窗口，如图 3-16 所示。

（4）单击“确定”按钮，系统密钥建立完成，在 Swriter.exe 的当前目录下生成一个文件名为 PK.txt 的文件，如图 3-17 所示，其中的内容包括自己的加密基数和公开密钥，可以将该文件发送给需要与其通信的人，让他将其中的内容添加到其通信密钥簿中。



图 3-15　生成/改变密钥窗口

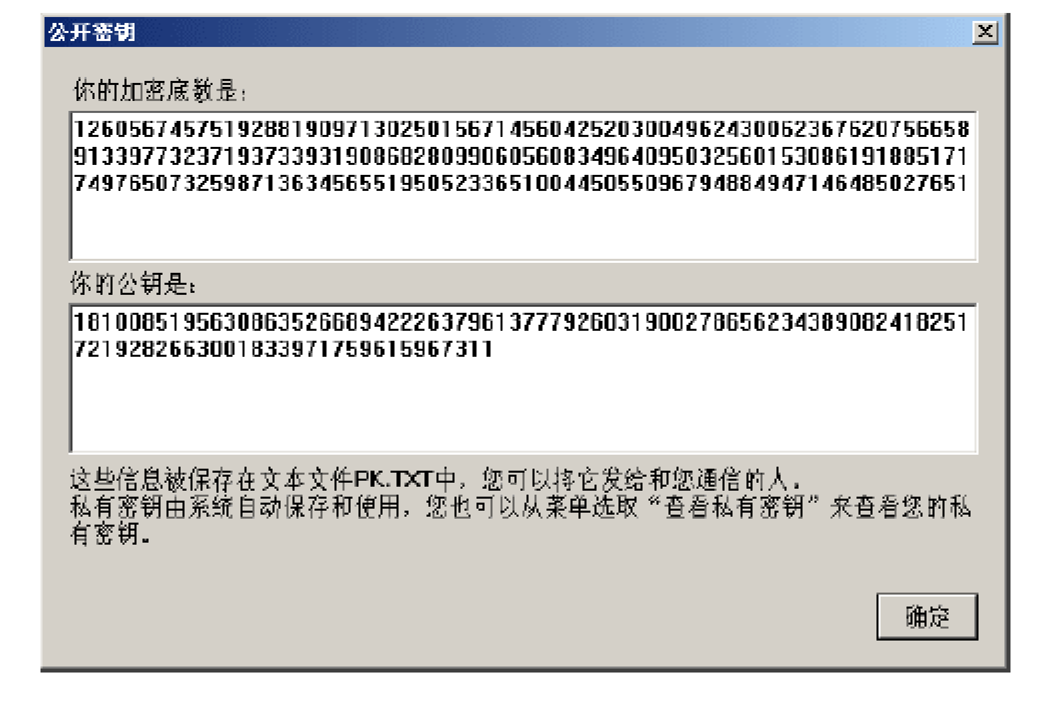


图 3-16　公开密钥窗口

（5）选择“密钥管理”|“通信密钥簿”命令，出现“通信密钥簿”对话框，如图 3-18 所示。

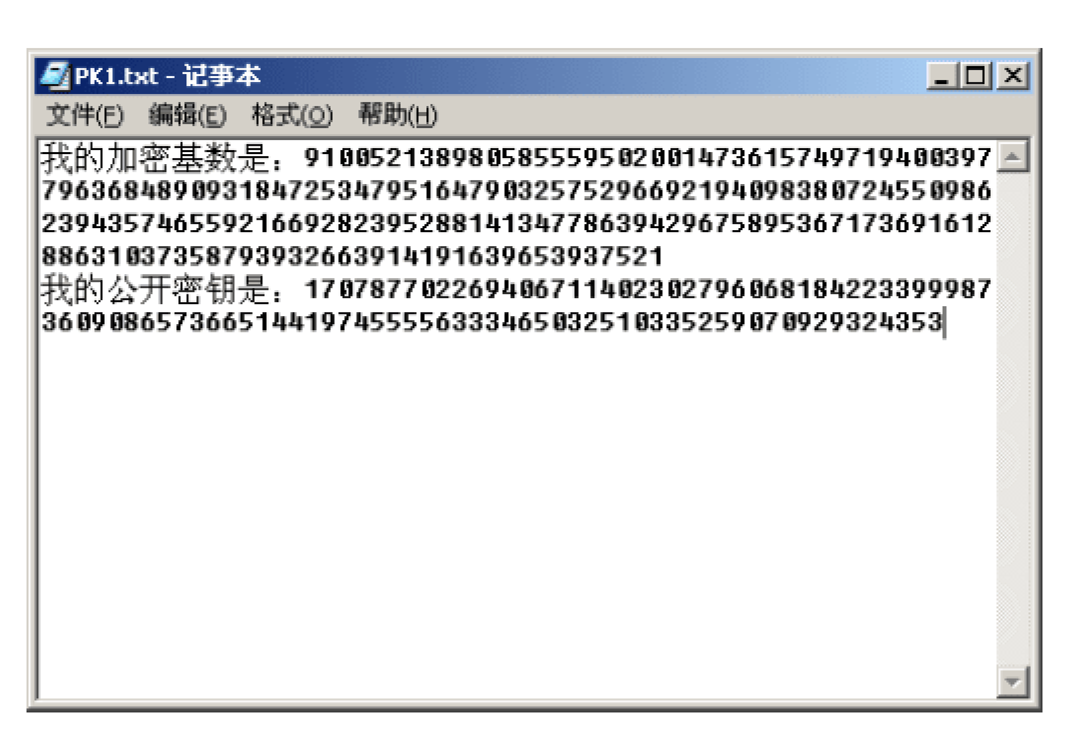


图 3-17　系统密钥加密基数和公钥

图 3-18　通信密钥簿

（6）在“通信密钥簿”窗口中，将来自其他人的密钥系统的加密基数和公钥以及姓名添加到通信密钥簿中。

2．加密文件

加密文件的过程就是用对方给的公钥来加密文件，加密文件的基本操作步骤如下。

（1）在 Swriter 启动以后，在窗口中输入需要加密的信息，如图 3-19 所示。

（2）单击工具栏上的“保存”按钮，系统提示是否需要对文件信息进行加密，提示对话框如图 3-20 所示。

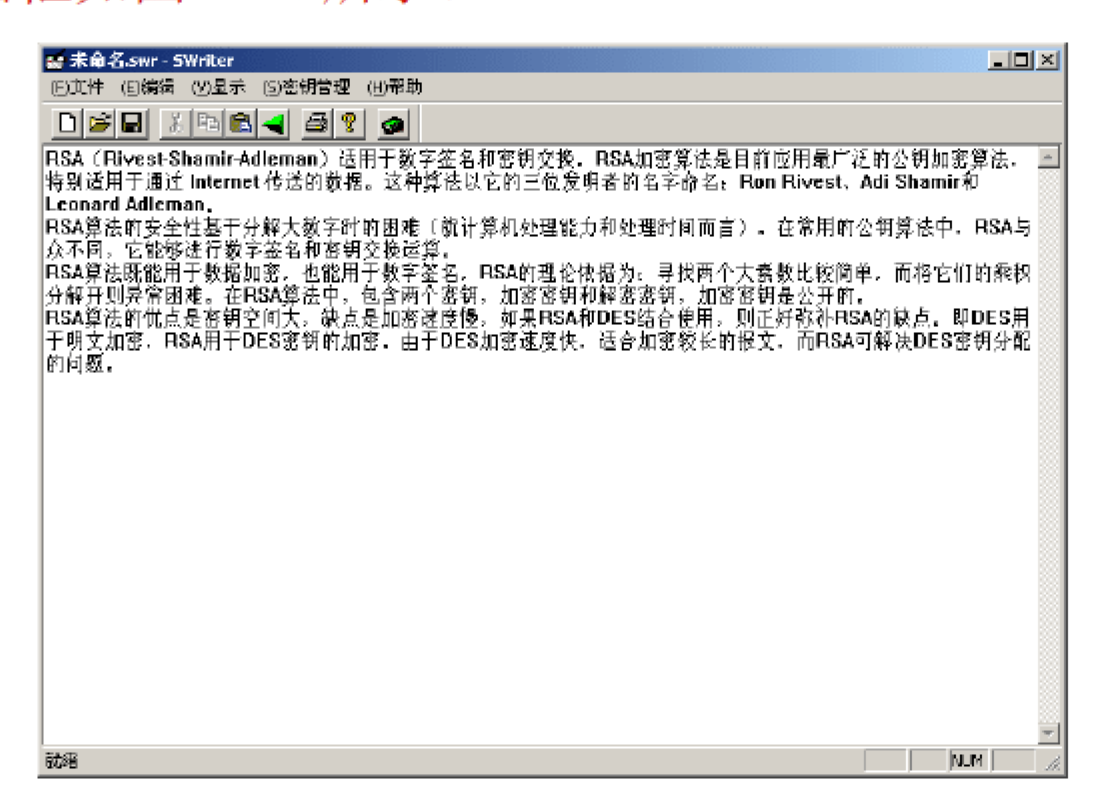


图 3-19　输入需要加密的信息



图 3-20　是否加密提示对话框

（3）为了保证信息的安全，单击“是”按钮，出现“加密保存”对话框，这里可以对

文件的加密信息进行设置，如图 3-21 所示。

（4）在“加密给”列表框中，选择需要将文档发送给某人就选择某人，这样文档就可以根据他所提供的公钥进行加密，当文档发送给他时，他就可以用自己的私钥进行解密，这里选择 sales，选中“不可否认性（数字签名）”，然后单击“确定”按钮，将文件保存到硬盘上。

3．解密文件

解密文件就是别人用我们的公钥对文件加密后发送给我们，然后我们再用我们的私钥对加密文件进行解密，具体操作步骤如下。

（1）双击接收到的加密文件，出现提示对话框，提示是否需要解密，如图 3-22 所示。

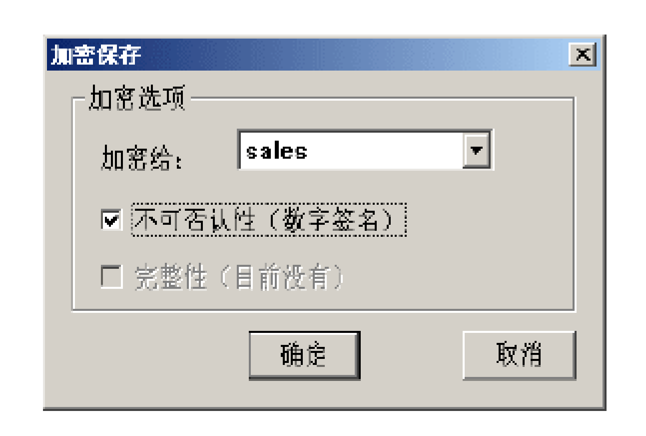


图 3-21　加密设置



图 3-22　提示密文是否解密

（2）单击“是”按钮，要求选择发送者的姓名，如图 3-23 所示。

（3）因为该文档是 sales 发送来的，所以这里选择 sales，然后单击“确定”按钮，看到文档的内容，如图 3-24 所示。



图 3-23　选择信件来源

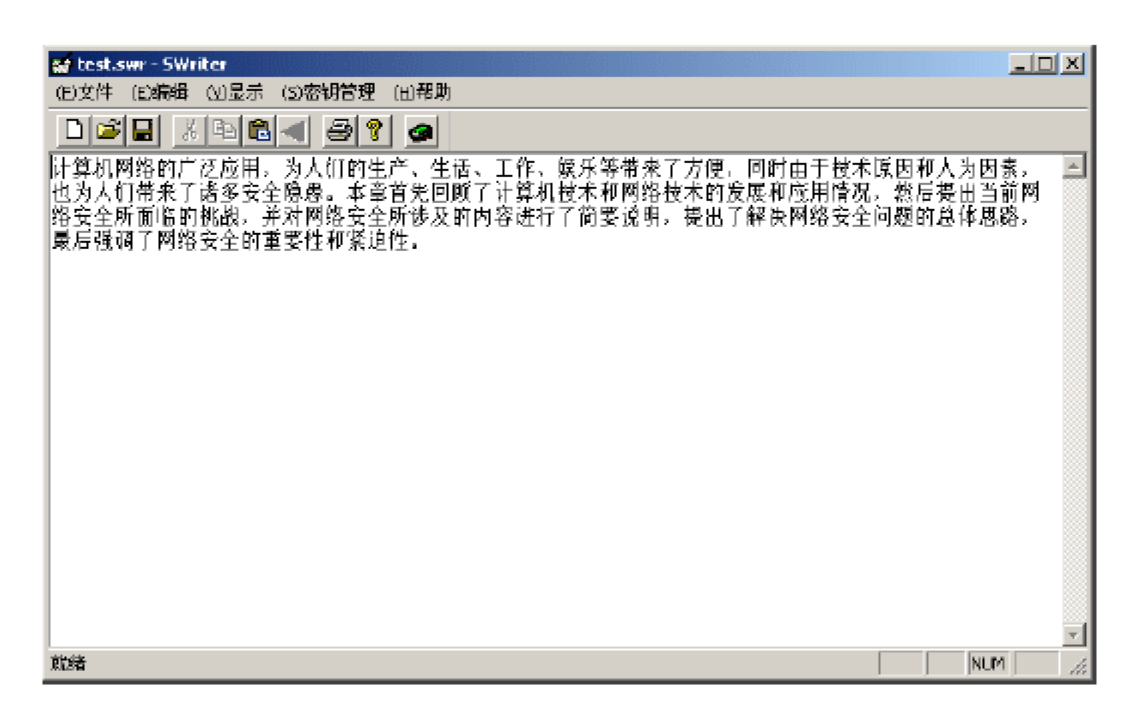


图 3-24　解密后的文档内容

（4）如果在第一步单击“否”按钮，将得到密文，如图 3-25 所示，可以看出显示的是加密过的内容。

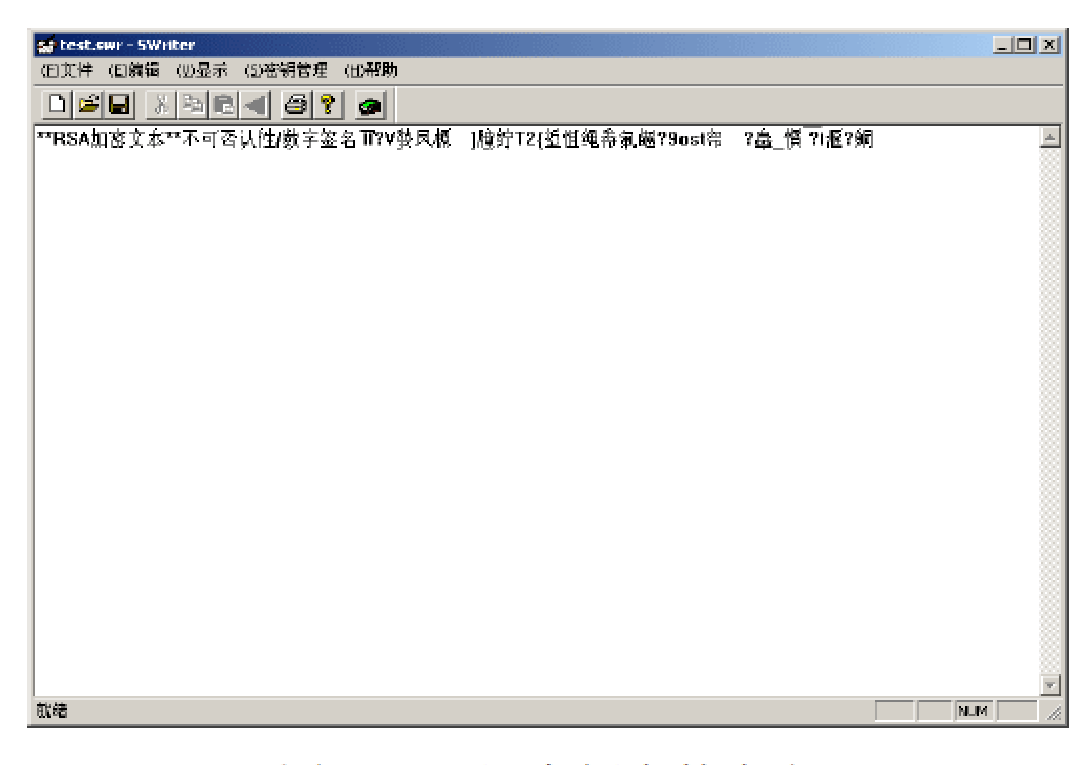


图 3-25　没有解密的密文

（5）通过解密后的内容和解密前的内容对比，可以看出两者之间无法看出关系。

通过上述的建立密钥、加密文件和解密文件三个过程，就可以实现文件的安全传输了，因为私钥不会在网络上传输，从而保证该加密算法可以有效防止网络偷听的方式来破解文件的密码。

3.4　数据加密技术的应用

从保护数据的角度讲，数据加密技术的应用主要可以分为三部分，即数据加密、数据传输安全和身份认证管理。

（1）数据加密就是按照确定的密码算法将敏感的明文数据变换成难以识别的密文数据，通过使用不同的密钥，可用同一加密算法将同一明文加密成不同的密文。当需要时，可使用密钥将密文数据还原成明文数据，称为解密。这样就可以实现数据的保密性。数据加密被公认为是保护数据传输安全唯一实用的方法和保护存储数据安全的有效方法，它是数据保护在技术上最重要的防线。

（2）数据传输安全是指数据在传输过程中必须要确保数据的安全性、完整性和不可篡改性。

（3）身份认证的目的是确定系统和网络的访问者是否是合法用户。主要采用登录密码、代表用户身份的物品（如智能卡、IC 卡等）或反映用户生理特征的标识鉴别访问者的身份。

3.4.1　数据加密

数据加密技术是最基本的安全技术，被誉为信息安全的核心，最初主要用于保证数据在存储和传输过程中的保密性。它通过变换和置换等各种方法将被保护信息置换成密文，然后再进行信息的存储或传输，即使加密信息在存储或者传输过程为非授权人员所获得，也可以保证这些信息不为其认知，从而达到保护信息的目的。该方法的保密性直接取决于所采用的密码算法和密钥长度。

根据密钥类型不同可以将现代密码技术分为两类：对称加密算法（私钥密码体系）和非对称加密算法（公钥密码体系）。在对称加密算法中，数据加密和解密采用的都是同一个密钥，因而其安全性依赖于所持有密钥的安全性。对称加密算法的主要优点是加密和解密速度快，加密强度高，且算法公开，但其最大的缺点是实现密钥的秘密分发困难，在大量用户的情况下密钥管理复杂，而且无法完成身份认证等功能，不便于应用在网络开放的环境中。目前最著名的对称加密算法有数据加密标准 DES 和欧洲数据加密标准 IDEA 等，目前加密强度最高的对称加密算法是高级加密标准 AES。

对称加密算法、非对称加密算法和不可逆加密算法可以分别应用于数据加密、身份认证和数据安全传输。

1．对称加密算法

对称加密算法是应用较早的加密算法，技术成熟。在对称加密算法中，数据发信方将明文（原始数据）和加密密钥一起经过特殊加密算法处理后，使其变成复杂的加密密文发送出去。收信方收到密文后，若想解读原文，则需要使用加密用过的密钥及相同算法的逆算法对密文进行解密，才能使其恢复成可读明文。在对称加密算法中，使用的密钥只有一

个，发收信双方都使用这个密钥对数据进行加密和解密，这就要求解密方事先必须知道加密密钥。对称加密算法的特点是算法公开、计算量小、加密速度快、加密效率高。不足之处是，交易双方都使用同样钥匙，安全性得不到保证。此外，每对用户每次使用对称加密算法时，都需要使用其他人不知道的唯一钥匙，这会使得发收信双方所拥有的钥匙数量呈几何级数增长，密钥管理成为用户的负担。对称加密算法在分布式网络系统上使用较为困难，主要是因为密钥管理困难，使用成本较高。在计算机专网系统中广泛使用的对称加密算法有 DES、IDEA 和 AES。

传统的 DES 由于只有 56 位的密钥，因此已经不适应当今分布式开放网络对数据加密安全性的要求。1997 年 RSA 数据安全公司发起了一项“DES 挑战赛”的活动，志愿者 4 次分别用 4 个月、41 天、56 个小时和 22 个小时破解了其用 56 位密钥 DES 算法加密的密文。即 DES 加密算法在计算机速度提升后的今天被认为是不安全的。

AES 是美国联邦政府采用的商业及政府数据加密标准，预计将在未来几十年里代替 DES 在各个领域中得到广泛应用。AES 提供 128 位密钥，因此，128 位 AES 的加密强度是 56 位 DES 加密强度的 1021 倍还多。假设可以制造一部可以在 1 秒内破解 DES 密码的机器，那么使用这台机器破解一个 128 位 AES 密码需要大约 149 亿万年的时间。（更深一步比较而言，宇宙一般被认为存在了还不到 200 亿年）因此可以预计，美国国家标准局倡导的 AES 即将作为新标准取代 DES。

2．不对称加密算法

不对称加密算法使用两把完全不同但又是完全匹配的一对钥匙——公钥和私钥。在使用不对称加密算法加密文件时，只有使用匹配的一对公钥和私钥，才能完成对明文的加密和解密过程。加密明文时采用公钥加密，解密密文时使用私钥才能完成，而且发信方（加密者）知道收信方的公钥，只有收信方（解密者）才是唯一知道自己私钥的人。不对称加密算法的基本原理是，如果发信方想发送只有收信方才能解读的加密信息，发信方必须首先知道收信方的公钥，然后利用收信方的公钥来加密原文；收信方收到加密密文后，使用自己的私钥才能解密密文。显然，采用不对称加密算法，收发信双方在通信之前，收信方必须将自己早已随机生成的公钥送给发信方，而自己保留私钥。由于不对称算法拥有两个密钥，因而特别适用于分布式系统中的数据加密。广泛应用的不对称加密算法有 RSA 算法和美国国家标准局提出的 DSA。以不对称加密算法为基础的加密技术应用非常广泛。

3．不可逆加密算法

不可逆加密算法的特征是加密过程中不需要使用密钥，输入明文后由系统直接经过加密算法处理成密文，这种加密后的数据是无法被解密的，只有重新输入明文，并再次经过同样不可逆的加密算法处理，得到相同的加密密文并被系统重新识别后，才能真正解密。显然，在这类加密过程中，加密是自己，解密还得是自己，而所谓解密，实际上就是重新加一次密，所应用的“密码”也就是输入的明文。不可逆加密算法不存在密钥保管和分发问题，非常适合在分布式网络系统上使用，但因加密计算复杂，工作量相当繁重，通常只在数据量有限的情形下使用，如广泛应用在计算机系统中的口令加密，利用的就是不可逆加密算法。近年来，随着计算机系统性能的不断提高，不可逆加密的应用领域正在逐渐增大。在计算机网络中应用较多不可逆加密算法的有 RSA 公司发明的 MD5 算法和由美国国家标准局建议的不可逆加密标准 SHS（Secure Hash Standard：安全杂乱信息标准）等。

3.4.2　传输安全

数据传输加密技术目的是对传输中的数据流加密，以防止通信线路上的窃听、泄露、篡改和破坏。数据传输的完整性通常通过数字签名的方式来实现，即数据的发送方在发送数据的同时利用单向的不可逆加密算法哈希函数或者其他信息文摘算法计算出所传输数据的消息文摘，并将该消息文摘作为数字签名随数据一同发送。接收方在收到数据的同时也收到该数据的数字签名，接收方使用相同的算法计算出接收到的数据的数字签名，并将该数字签名和接收到的数字签名进行比较，若二者相同，则说明数据在传输过程中未被修改，数据的完整性得到了保证。

哈希算法也称为消息摘要或单向转换，是一种不可逆加密算法，称它为单向转换是因为：

（1）双方必须在通信的两个端头处各自执行哈希函数计算；

（2）使用哈希函数很容易从消息计算出消息摘要，但其逆向反演过程以目前计算机的运算能力几乎不可实现。

哈希散列本身就是所谓加密检查，通信双方必须各自执行函数计算来验证消息。举例来说，发送方首先使用哈希算法计算消息检验和，然后将计算结果 A 封装进数据包中一起发送；接收方再对所接收的消息执行哈希算法计算得出结果 B，并将 B 与 A 进行比较。如果消息在传输中遭篡改致使 B 与 A 不一致，接收方丢弃该数据包。

有两种最常用的哈希函数：

（1）MD5（消息摘要 5）：MD5 对 MD4 做了改进，计算速度比 MD4 稍慢，但安全性能得到了进一步改善。MD5 在计算中使用了 64 个 32 位常数，最终生成一个 128 位的完整性检查和。

（2）SHA 安全哈希算法：其算法以 MD5 为原型。 SHA 在计算中使用了 79 个 32 位常数，最终产生一个 160 位完整性检验和。SHA 检验和长度比 MD5 更长，因此安全性也更高。

3.4.3　身份认证

身份认证要求参与安全通信的双方在进行安全通信前，必须互相鉴别对方的身份。保护数据不仅仅是要让数据正确、长久地存在，更重要的是，要让不该看到数据的人看不到。这方面，就必须依靠身份认证技术来给数据加上一把锁。数据存在的价值就是需要被合理访问，所以，建立信息安全体系的目的应该是保证系统中的数据只能被有权限的人访问，未经授权的人则无法访问到数据。如果没有有效的身份认证手段，访问者的身份就很容易被伪造，使得未经授权的人仿冒有权限人的身份，这样，任何安全防范体系就都形同虚设，所有安全投入就被无情地浪费了。

在企业管理系统中，身份认证技术要能够密切结合企业的业务流程，阻止对重要资源的非法访问。身份认证技术可以用于解决访问者的物理身份和数字身份的一致性问题，给其他安全技术提供权限管理的依据。所以说，身份认证是整个信息安全体系的基础。

由于网上的通信双方互不见面，必须在交易时（交换敏感信息时）确认对方的真实身份； 身份认证指的是用户身份的确认技术，它是网络安全的第一道防线，也是最重要的一

道防线。

在公共网络上的认证，从安全角度分有两类：一类是请求认证者的秘密信息（例如：口令）在网上传送的口令认证方式，另一类是使用不对称加密算法，而不需要在网上传送秘密信息的认证方式，这类认证方式中包括数字签名认证方式。

1. 口令认证方式

口令认证必须具备一个前提：请求认证者必须具有一个 ID，该 ID 必须在认证者的用户数据库（该数据库必须包括 ID 和口令）中是唯一的。同时为了保证认证的有效性必须考虑到以下几个问题。

（1）求认证者的口令必须是安全的。

（2）在传输过程中，口令不能被窃看、替换。

（3）请求认证者在向认证者请求认证前，必须确认认证者的真实身份，否则会把口令发给冒充的认证者。

口令认证方式还有一个最大的安全问题就是系统的管理员通常都能得到所有用户的口令。因此，为了避免这样的安全隐患，通常情况下会在数据库中保存口令的哈希值，通过验证哈希值的方法来认证身份。

2. 使用不对称加密算法的认证方式 （数字证书方式）

使用不对称加密算法的认证方式，认证双方的个人秘密信息（例如：口令）不用在网络上传送，减少了认证的风险。这种方式是通过请求认证者与认证者之间对一个随机数作数字签名与验证数字签名来实现的。

认证一旦通过，双方即建立安全通道进行通信，在每一次的请求和响应中进行，即接受信息的一方先从接收到的信息中验证发信人的身份信息，验证通过后才根据发来的信息进行相应的处理。

用于实现数字签名和验证数字签名的密钥对必须与进行认证的一方唯一对应 。

在公钥密码（不对称加密算法）体系中，数据加密和解密采用不同的密钥，而且用加密密钥加密的数据只有采用相应的解密密钥才能解密，更重要的是从加密密码来求解解密密钥十分困难。在实际应用中，用户通常将密钥对中的加密密钥公开（称为公钥），而秘密持有解密密钥（称为私钥）。利用公钥体系可以方便地实现对用户的身份认证，也即用户在信息传输前首先用所持有的私钥对传输的信息进行加密，信息接收者在收到这些信息之后利用该用户向外公布的公钥进行解密，如果能够解开，说明信息确实为该用户所发送，这样就方便地实现了对信息发送方身份的鉴别和认证。在实际应用中通常将公钥密码体系和数字签名算法结合使用，在保证数据传输完整性的同时完成对用户的身份认证。

目前的不对称加密算法都是基于一些复杂的数学难题，例如目前广泛使用的 RSA 算法就是基于大整数因子分解这一著名的数学难题。目前常用的非对称加密算法包括整数因子分解（以 RSA 为代表）、椭圆曲线离散对数和离散对数（以 DSA 为代表）。公钥密码体系的优点是能适应网络的开放性要求，密钥管理简单，并且可方便地实现数字签名和身份认证等功能，是目前电子商务等技术的核心基础。其缺点是算法复杂，加密数据的速度和效率较低。因此在实际应用中，通常将对称加密算法和非对称加密算法结合使用，利用 AES、DES 或者 IDEA 等对称加密算法来进行大容量数据的加密，而采用 RSA 等非对称加密算法来传递对称加密算法所使用的密钥，通过这种方法可以有效地提高加密的效率并能简化对

密钥的管理。

3.4.4　在电子商务方面的应用

电子商务（E-business）要求顾客可以在网上进行各种商务活动，不必担心自己的信用卡会被人盗用。在过去，用户为了防止信用卡的号码被窃取，一般是通过电话订货，然后使用用户的信用卡进行付款。现在人们开始用 RSA（一种公开/私有密钥）的加密技术，提高信用卡交易的安全性，从而使电子商务走向实用成为可能。

许多人都知道 NETSCAPE 公司是 Internet 商业中领先技术的提供者，该公司提供了一种基于 RSA 和保密密钥的应用于因特网的技术，被称为安全套接字层（Secure Sockets Layer，SSL）。

也许很多人知道 Socket，它是一个编程界面，并不提供任何安全措施，而 SSL 不但提供编程界面，而且向上提供一种安全的服务，SSL3.0 现在已经应用到了服务器和浏览器上，SSL2.0 则只能应用于服务器端。

SSL3.0 用一种电子证书来实行身份进行验证后，双方就可以用保密密钥进行安全的会话了。它同时使用“对称”和“非对称”加密方法，在客户与电子商务的服务器进行沟通的过程中，客户会产生一个会话密钥，然后客户用服务器端的公钥将会话密钥进行加密，再传给服务器端，在双方都知道会话密钥后，传输的数据都是以会话密钥进行加密与解密的，但服务器端发给用户的公钥必需先向有关发证机关申请，以得到公证。

基于 SSL3.0 提供的安全保障，用户就可以自由订购商品并且给出信用卡号了，也可以在网上和合作伙伴交流商业信息并且让供应商把订单和收货单从网上发过来，这样可以节省大量的纸张，为公司节省大量的电话、传真费用。在过去，电子信息交换（Electric Data Interchange，EDI）、信息交易（information transaction）和金融交易（financial transaction）都是在专用网络上完成的，使用专用网的费用大大高于互联网。正是这样巨大的诱惑，才使人们开始发展因特网上的电子商务，但不要忘记数据加密。

3.4.5　加密技术在 VPN 中的应用

现在，越多越多的公司走向国际化，一个公司可能在多个国家都有办事机构或销售中心，每一个机构都有自己的局域网，但在当今的网络社会人们的要求不仅如此，用户希望将这些局域网连接在一起组成一个公司的广域网，这个在现在已不是什么难事了。

事实上，很多公司都已经这样做了，但他们一般使用租用专用线路来连接这些局域网，他们考虑的就是网络的安全问题。现在具有加密/解密功能的路由器已到处都是，这就使人们通过互联网连接这些局域网成为可能，这就是我们通常所说的虚拟专用网（Virtual Private Network,VPN）。当数据离开发送者所在的局域网时，该数据首先被用户端连接到互联网上的路由器进行硬件加密，数据在互联网上是以加密的形式传送的，当达到目的 LAN 的路由器时，该路由器就会对数据进行解密，这样目的 LAN 中的用户就可以看到真正的信息了。

3.5　加密举例

为了能够更加形象地对加密和解密过程进行理解，这里通过常用的 Word 文档的加密

和解密过程来做说明。

Word 文档的加密过程如下。

（1）选择“开始”|“程序”| Microsoft Office | Microsoft Word 命令，Word 编辑窗口出现，在窗口中输入一些文字信息，如图 3-26 所示。

（2）将文档保存到一个任意一个目录，这里为了方便，我们选择保存到“我的文档”中，如图 3-27 所示。

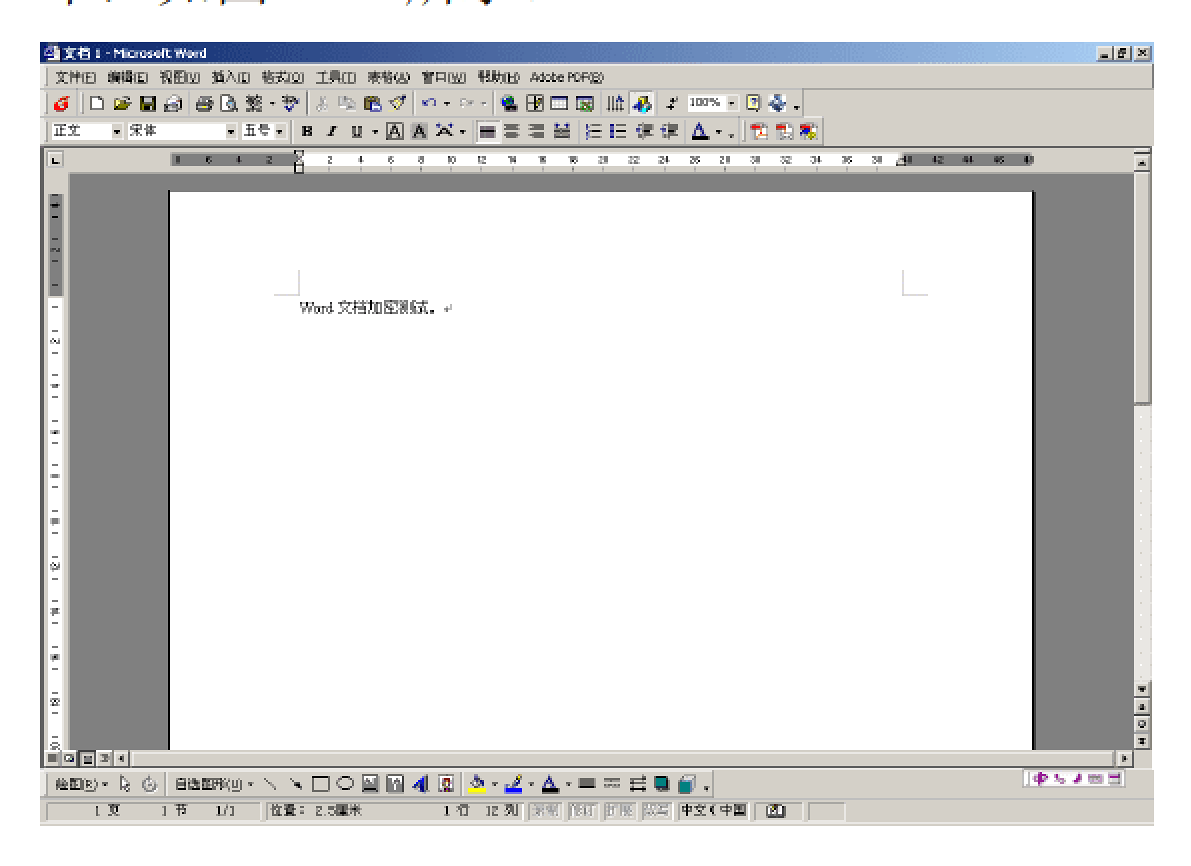


图 3-26 Word 文档编辑界面

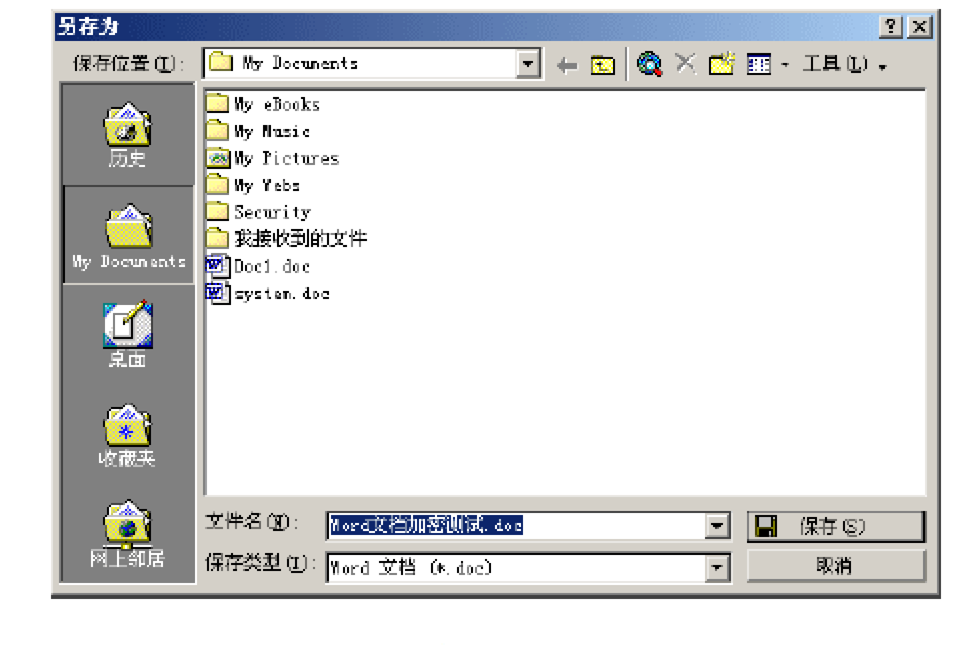


图 3-27 保存 Word 文档

（3）用 UltraEdit-32 工具（可以用 16 进制形式打开文件）打开刚才保存的 Word 文档，可以看到文档的内容，此时的 Word 文档没有被加密，如图 3-28 所示。

（4）用 Word 打开刚才的 Word，选择“工具”|“选项”命令，出现“选项”对话框，在“选项”对话框中，选择“保存”选项卡，如图 3-29 所示。

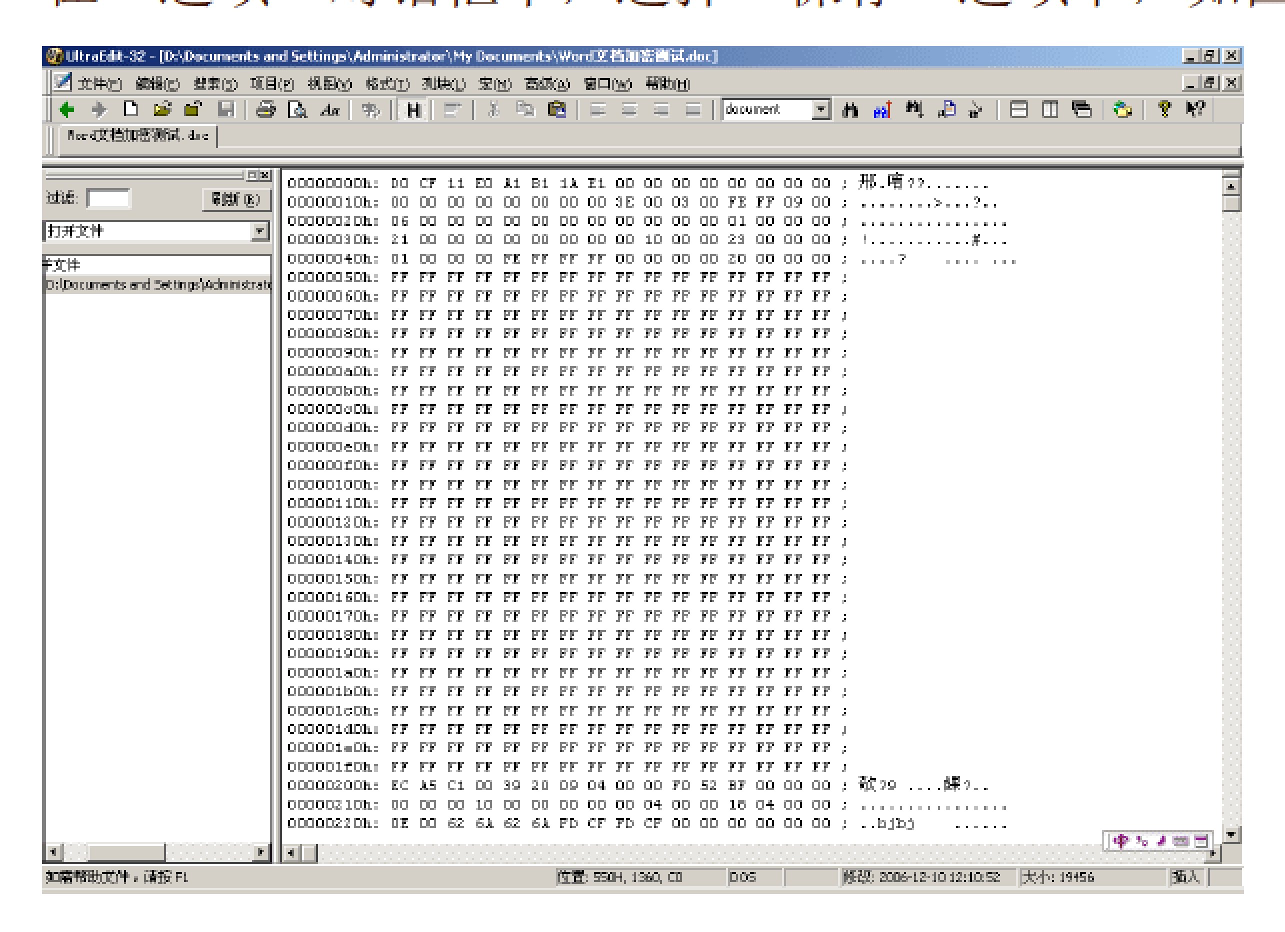


图 3-28 Word 文档的二进制形式

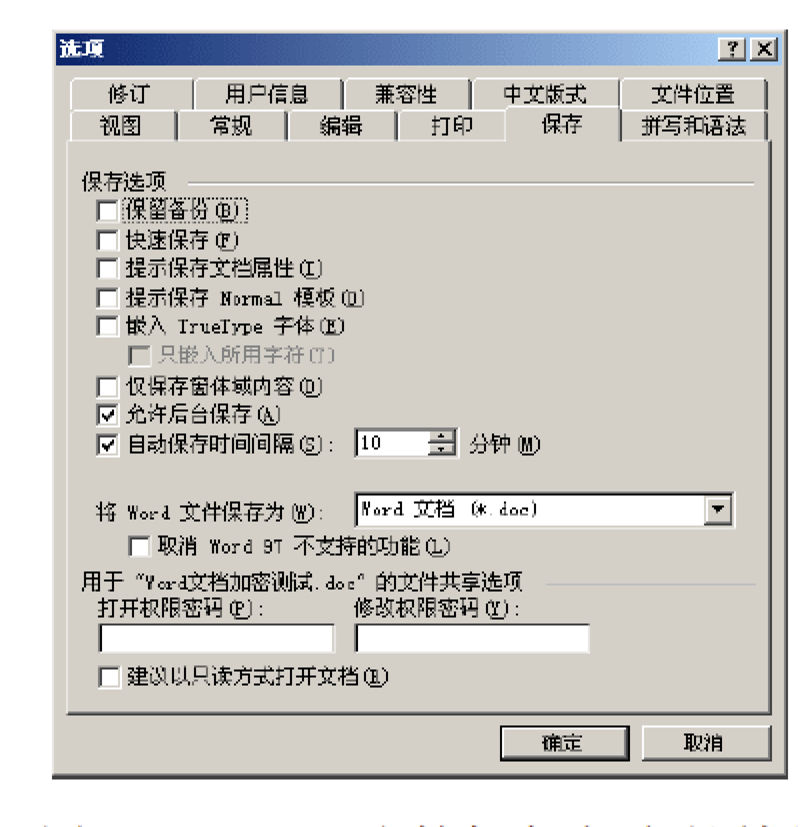


图 3-29 Word 文档保存选项对话框

（5）在“打开权限密码”文本框和“修改权限密码”文本框中输入密码，然后单击“确定”按钮，出现“确认密码”对话框，要求再次输入刚才设置的“打开权限密码”，如图 3-30 所示。

（6）输入确认打开权限密码以后，单击“确定”按钮，再次出现“确认密码”对话框，要求再次输入刚才设置的“修改权限密码”，如图 3-31 所示。

（7）单击“确认密码”对话框中的“确定”按钮，单击“选项”对话框中的“确定”按钮，完成对 Word 文档的加密，关闭 Word 文档。

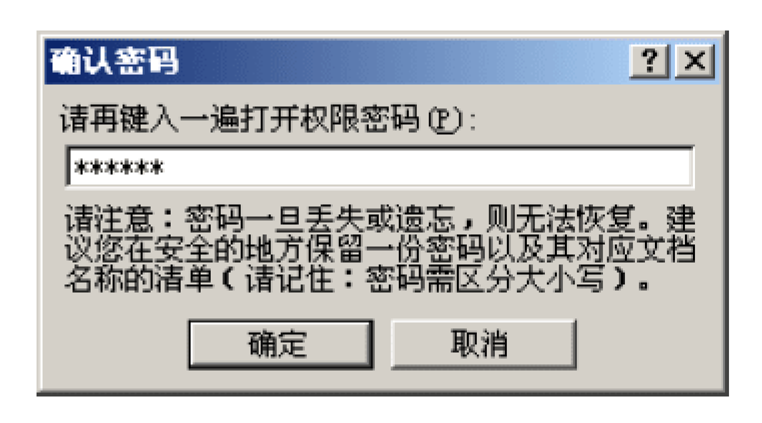



图 3-30　确认打开权限密码对话框

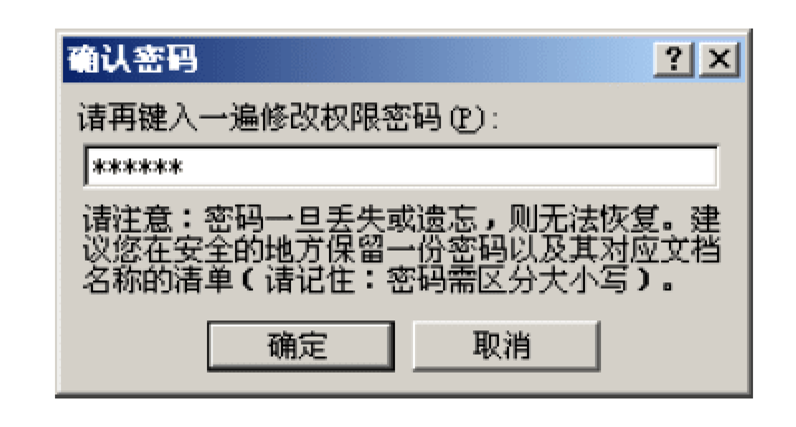


图 3-31　确认修改权限密码对话框

（8）重新用 Word 打开刚才加密过的文档，出现“密码”对话框，Word 要求输入打开权限密码，出现如图 3-32 所示。

（9）输入刚才设置的打开权限密码，然后单击“确定”按钮，出现第二个“密码”对话框，要求输入修改权限密码，此时有两个选择，如果需要修改文件内容，需要输入密码，然后单击“确定”按钮，如果不需要修改文件内容，可以单击“只读”按钮，同样可以打开文档，只是此时不能对文档进行修改，如图 3-33 所示。

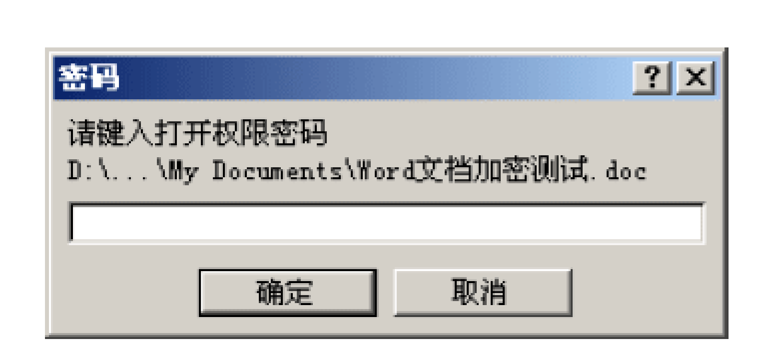


图 3-32　输入打开权限密码窗口

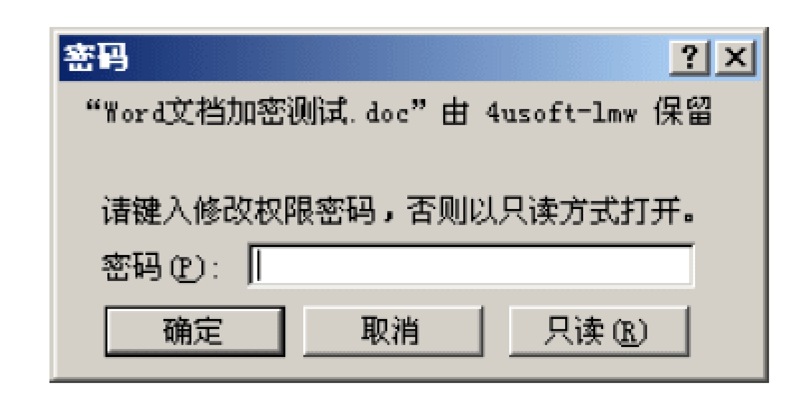


图 3-33　输入修改权限密码窗口

（10）Word 文档打开后，出现文档编辑窗口。

（11）用 UltraEdit-32 工具打开刚才加密过的 Word 文档，可以看到文档的内容，此时的 Word 文档已经被加密，如图 3-34 所示。

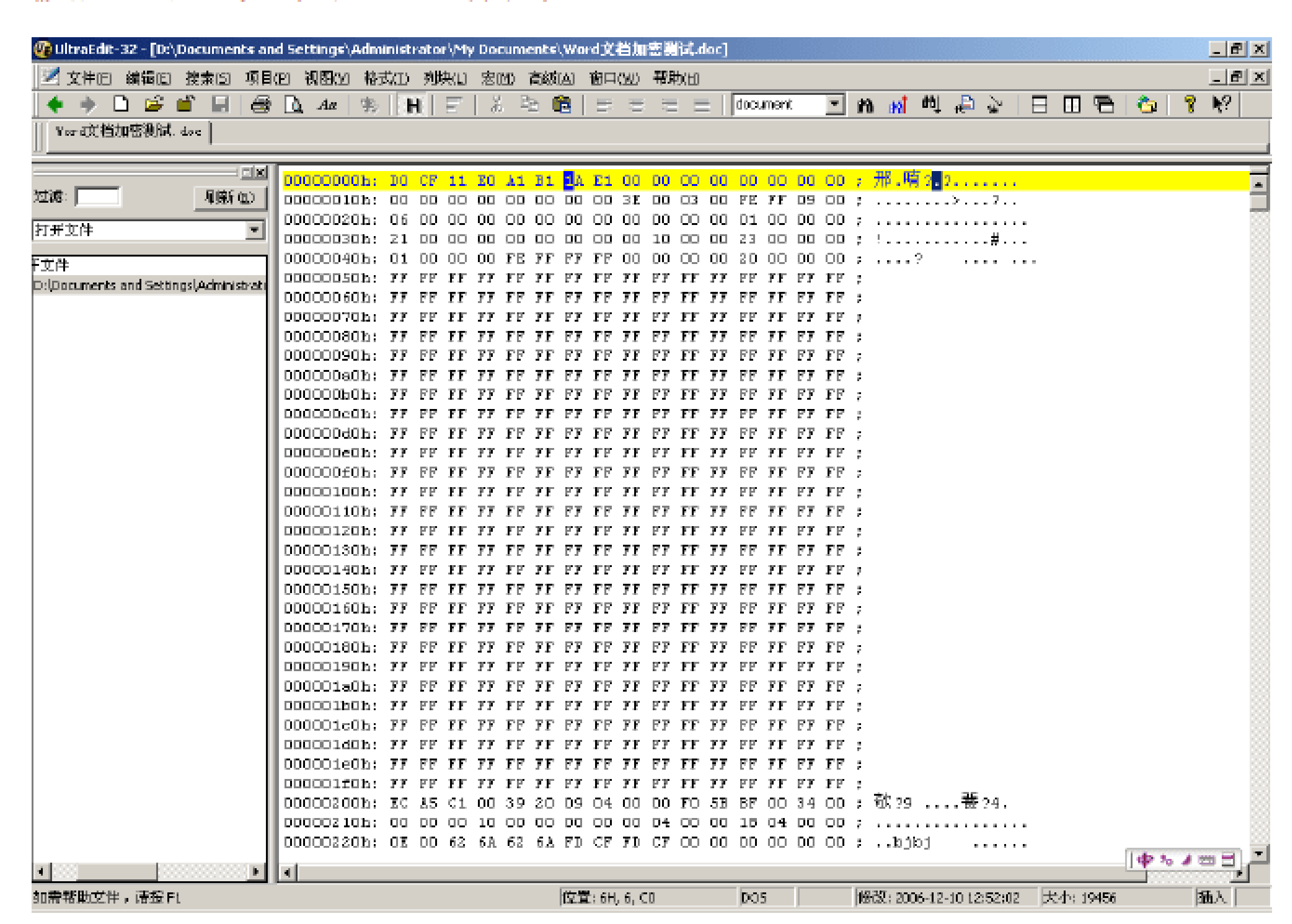


图 3-34　加密过的 Word 文档

（12）可以看出加密后的内容和加密前的内容有所不同。

Word 文档的解密过程如下。

（1）用 Word 打开刚才加密过的文件，选择“工具”|“选项”命令，出现“选项”对话框，在对话框中选择“保存”选项卡，如图 3-35 所示。

（2）将“打开权限密码”文本框和“修改权限密码”文本框中的密码删除，然后单击“确定”按钮，然后再单击工具栏上的“保存”按钮保存 Word 文件的内容，这样就完成

对 Word 文档的解密了。

（3）用 UltraEdit-32 工具打开刚才解密过的 Word 文档，可以看到文档的内容，此时的 Word 文档已经被解密，如图 3-36 所示。

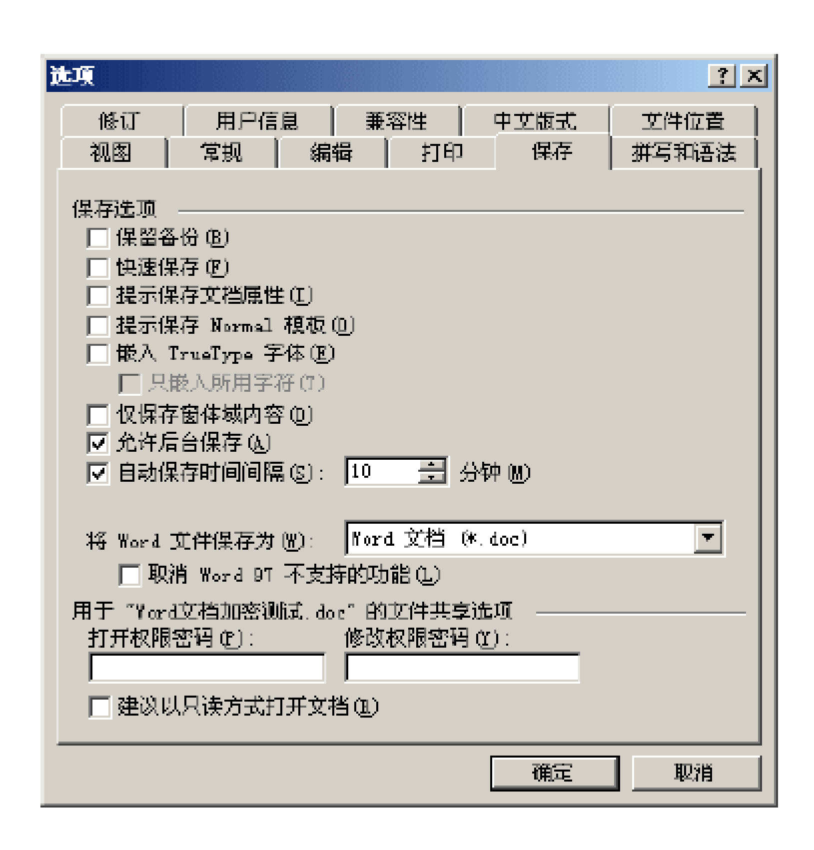


图 3-35 “选项”对话框

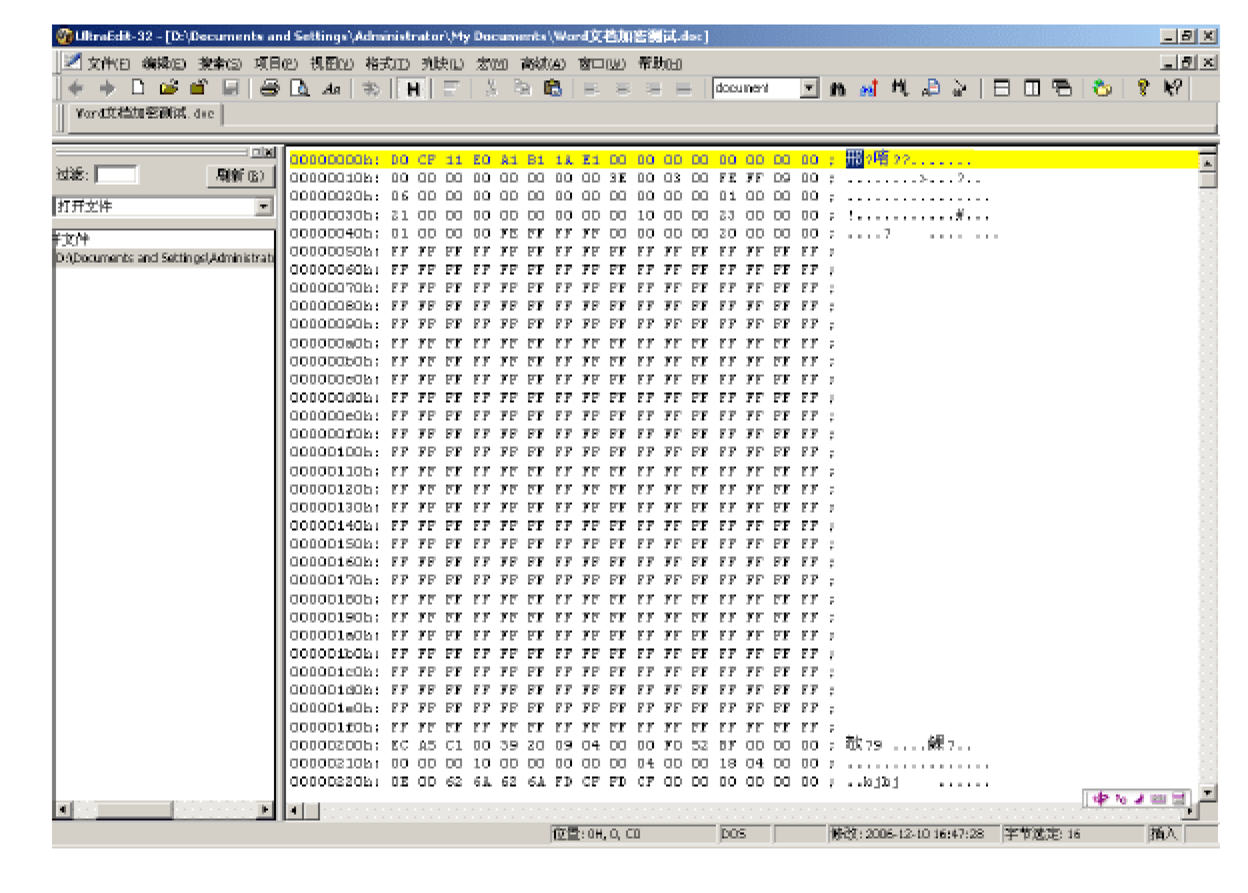


图 3-36 解密后的 Word 文档

（4）可以看出 Word 文档已经被解密，和加密以前的内容是完全一样的，再次打开这个文档的时候也不会要求输入密码。

习题

1．数据加密技术包括哪些相关技术？
2．简述对称加密算法的基本思想。
3．简述公开密钥算法的基本思想。
4．简述数据加密技术的应用。
5．用一个加密工具给一个 Word 文件加密。

第 4 章　防火墙技术

教学提示

随着计算机技术应用的普及，各个组织机构的运行越来越依赖和离不开计算机，各种业务的运行架构于现代化的网络环境中。企业计算机系统作为信息化程度较高、计算机网络应用情况比较先进的一个特殊系统，其业务也同样地越来越依赖于计算机。保证业务系统和工作的正常、可靠和安全地进行是信息系统工作的一个重要话题，所以防火墙作为网络安全的一个重要组成部分被广泛地使用。

在网络安全的所有工具中，防火墙是保护内部网络安全，防止外部攻击的最有效的工具。为了充分认识、理解并应用好该工具，本章将对防火墙技术的相关知识进行讲解，具体内容包括防火墙的基本概念、防火墙的功能、防火墙的分类以及各种类型防火墙的特点、防火墙的选择原则以及防火墙技术的发展情况。

防火墙作为网络安全体系结构中的一个不可缺少的组成部分，对于整个网络系统的安全具有重要作用。通过对本章内容的学习，深入了解防火墙的技术原理、功能以及各种防火墙的特点和选择原则以及发展趋势等，对于构建安全的网络系统具有重要的意义。

教学重点

- 防火墙的工作原理。
- 防火墙技术分类及其特点。
- 防火墙体系结构。
- 分布式防火墙技术。
- 防火墙选择原则。
- 防火墙技术发展趋势。

4.1　防火墙基本概念

Internet 的迅速发展提供了发布信息和检索信息的场所，但也带来了信息污染和信息破坏的危险，人们为了保护其数据和资源的安全，部署了防火墙。防火墙本质上是一种保护装置，它保护数据、资源和用户的声誉。

4.1.1　防火墙定义

防火墙的本义原是指古代人们房屋之间修建的那道墙，这道墙可以防止火灾发生的时候蔓延到别的房屋。而这里所说的防火墙当然不是指物理上的防火墙，而是指隔离在本地网络与外界网络之间的一道防御系统，是这一类防范措施的总称。

防火墙是一个或一组在两个网络之间执行访问控制策略的系统，包括硬件和软件，目的是保护网络不被可疑人侵扰。本质上，它遵从的是一种允许或阻止业务来往的网络通信

安全机制，也就是提供可控的过滤网络通信，只允许授权的通信。

通常，防火墙就是位于内部网或 Web 站点与 Internet 之间的一个路由器或一台计算机（又称为堡垒主机），其目的如同一个安全门，为门内的部分提供安全，控制那些允许出入应该受到保护的人或物。就像工作在门前的安全卫士，控制并检查站点的访问者。

防火墙是由管理员为保护自己的网络免遭外界非授权访问但又允许与 Internet 连接而发展起来的，从网际角度，防火墙可以看成是安装在两个网络之间的一道栅栏，根据安全计划和安全策略中的定义来保护其后面的网络，由软件和硬件组成的防火墙应该具有以下功能：

- 所有进出网络的通信流都应该通过防火墙；
- 所有穿过防火墙的通信流都必须有安全策略和计划的确认和授权；
- 理论上说，防火墙是穿不透的。

利用防火墙能保护站点不被任意连接，甚至能建立跟踪工具，帮助总结并记录有关正在进行的连接资源、服务器提供的通信量以及试图闯入者的任何企图。

总之，防火墙是阻止外面的人对你的网络进行访问的安全设备，此设备通常是软件和硬件的组合体，它通常根据一些规则来挑选想要或不想要的地址。

随着 Internet 上越来越多的用户访问 Web，运行例如 Telnet、FTP 和 Internet Mail 之类的服务，系统管理者和 LAN 管理者必须能够在提供访问的同时，保护他们的内部网，不给闯入者留有可乘之机。需要防范的三种基本进攻如下：

- 间谍：试图偷走敏感信息的黑客、入侵者和闯入者；
- 盗窃：盗窃对象包括数据、Web 表格、磁盘空间、CPU 资源、连接等；
- 破坏系统：通过路由器或主机／服务器蓄意破坏文件系统或阻止授权用户访问内部网、外部网或服务器。

这里，防火墙的作用是保护 Web 站点和公司的内部网，使之免遭 Internet 上各种危险的侵犯。

典型的防火墙建立在一个服务器／主机机器上，亦称“堡垒”，是一个多边协议路由器，这个堡垒有两个网络连接：一边与内部网相连，另一边与 Internet 相连。它的主要作用除了防止未经授权的来自 Internet 或对 Internet 的访问外，还包括为安全管理提供详细的系统活动的记录。在有的配置中，这个堡垒主机经常作为一个公共 Web 服务器或一个 FTP 或 E-mail 服务器使用。

通过在防火墙上运行的专门 HTTP 服务器，可使用“代理”服务器，以访问防火墙的另一边的 Web 服务器。

4.1.2 防火墙的功能

防火墙作为连接内部网络和外部网络的主要网络安全设备，主要具有以下几个方面的功能。

1. 防火墙是网络安全的屏障

一个防火墙（作为阻塞点、控制点）能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议进出受保护的网

络，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2．防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如在网络访问时，一次一密口令系统和其他的身份认证系统完全可以不必分散在各个主机上，而集中在防火墙身上。

3．对网络存取和访问进行监控审计

如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是非常重要的。首先的理由是可以清楚地知道防火墙是否能够抵挡攻击者的探测和攻击，并且清楚地知道防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

4．防止内部信息的外泄

通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透露内部细节如 Finger，DNS 等服务。Finger 显示了主机的所有用户的注册名、真名，最后登录时间和使用 shell 类型等。但是 Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时引起注意等等。防火墙可以同样阻塞有关内部网络中的 DNS 信息，这样一台主机的域名和 IP 地址就不会被外界所了解。

除了安全作用，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN。通过 VPN，将企事业单位在地域上分布在全世界各地的 LAN 或专用子网，有机地连成一个整体。不仅省去了专用通信线路，而且为信息共享提供了技术保障。

4.1.3　防火墙的分类

根据物理特性，防火墙分为两大类，硬件防火墙和软件防火墙。软件防火墙是一种安装在负责内外网络转换的网关服务器或者独立的个人计算机上的特殊程序，它是以逻辑形式存在的，防火墙程序跟随系统启动，通过运行在 ring0 级别的特殊驱动模块把防御机制插入系统关于网络的处理部分和网络接口设备驱动之间，形成一种逻辑上的防御体系。

在没有软件防火墙之前，系统和网络接口设备之间的通道是直接的，网络接口设备通过网络驱动程序接口（network driver interface specification，ndis）把网络上传来的各种报文都忠实地交给系统处理，例如一台计算机接收到请求列出机器上所有共享资源的数据报文，网络驱动程序接口直接把这个报文提交给系统，系统在处理后就会返回相应数据，在某些情况下就会造成信息泄露。而使用软件防火墙后，尽管 ndis 接收到的仍然是原封不动

的数据报文，但是在提交到系统的通道上多了一层防御机制，所有数据报文都要经过这层机制根据一定的规则判断处理，只有它认为安全的数据才能到达系统，其他数据则被丢弃。因为有规则提到“列出共享资源的行为是危险的”，因此在防火墙的判断下，这个报文会被丢弃，这样一来，系统接收不到报文，则认为什么事情也没有发生过，也就不会把信息泄露出去了。

软件防火墙工作于系统接口与网络驱动程序接口之间，用于检查过滤由网络驱动程序接口发送过来的数据，在无需改动硬件的前提下便能实现一定强度的安全保障，但是由于软件防火墙自身属于运行于系统上的程序，不可避免地需要占用一部分 CPU 资源维持工作，而且由于数据判断处理需要一定的时间，在一些数据流量大的网络里，软件防火墙会使整个系统工作效率和数据吞吐速度下降，甚至有些软件防火墙会存在漏洞，导致有害数据可以绕过它的防御体系，给数据安全带来损失，因此，许多企业并不会考虑用软件防火墙方案作为公司网络的防御措施，而是使用看得见摸得着的硬件防火墙。

硬件防火墙是一种以物理形式存在的专用设备，通常架设于两个网络的连接处，直接从网络设备上检查过滤有害的数据报文，位于防火墙设备后端的网络或者服务器接收到的是经过防火墙处理过的相对安全的数据，不必另外分出 CPU 资源去进行基于软件架构的网络驱动程序接口数据检测，可以大大提高工作效率。

硬件防火墙一般是通过网线连接于外部网络接口与内部服务器或企业网络之间的设备，这里又另外派分出两种结构，一种是普通硬件级别防火墙，它拥有标准计算机的硬件平台和一些功能经过简化处理的 UNIX 系列操作系统和防火墙软件，这种防火墙措施相当于专门拿出一台计算机安装了软件防火墙，除了不需要处理其他事务以外，它毕竟还是一般的操作系统，因此有可能会存在漏洞和不稳定因素，安全性并不能做到最好；另一种是所谓的“芯片”级硬件防火墙，它采用专门设计的硬件平台，在上面搭建的软件也是专门开发的，并非流行的操作系统，因而可以达到较好的安全性能保障。但无论是哪种硬件防火墙，管理员都可以通过计算机连接上去设置工作参数。由于硬件防火墙的主要作用是把传入的数据报文进行过滤处理后转发到位于防火墙后面的网络中，因此它自身的硬件规格也是分档次的，尽管硬件防火墙已经足以实现比较高的信息处理效率，但是在一些对数据吞吐量要求很高的网络里，档次低的防火墙仍然会形成瓶颈，所以对于一些大企业而言，芯片级的硬件防火墙才是他们的首选。

为防火墙分类的方法很多，除了从形式上把它分为软件防火墙和硬件防火墙以外，还可以从技术上分为“包过滤型”、“应用代理型”和“状态监视型”三类；从结构上又分为单一主机防火墙、路由集成式防火墙和分布式防火墙三种；按工作位置分为边界防火墙、个人防火墙和混合防火墙；按防火墙性能分为百兆级防火墙和千兆级防火墙两类等。这里主要介绍的是技术方面的分类，即“包过滤型”、“应用代理型”和“状态监视型”防火墙技术。

传统意义上的防火墙技术分为三大类，“包过滤”（packet filtering）、“应用代理”（application proxy）和“状态监视”（stateful inspection），无论一个防火墙的实现过程多么复杂，归根结底都是在这三种技术的基础上进行功能扩展的。

1. 包过滤技术

包过滤是最早使用的一种防火墙技术，它的第一代模型是“静态包过滤”（static packet filtering），使用包过滤技术的防火墙通常工作在 OSI 模型中的网络层（network layer）上，

后来发展为更新的“动态包过滤”（dynamic packet filtering）增加了传输层（transport layer），简而言之，包过滤技术工作的地方就是各种基于 tcp/ip 协议的数据报文进出的通道，它把这两层作为数据监控的对象，对每个数据包的头部、协议、地址、端口、类型等信息进行分析，并与预先设定好的防火墙过滤规则（filtering rule）进行核对，一旦发现某个包的某个或多个部分与过滤规则匹配并且条件为“阻止”的时候，这个包就会被丢弃。

适当的设置过滤规则可以让防火墙工作得更安全有效，但是这种技术只能根据预设的过滤规则进行判断，一旦出现一个没有在设计人员意料之中的有害数据包请求，整个防火墙的保护就相当于摆设了。也许你会想，让用户自行添加不行吗？但是别忘了，要为普通计算机用户考虑，并不是所有人都了解网络协议的，如果防火墙工具出现了过滤遗漏问题，就只能等着被入侵了。一些公司采用定期从网络升级过滤规则的方法，这个创意固然可以方便一部分家庭用户，但是对相对比较专业的用户而言，却不见得就是好事，因为他们可能会根据自己的机器环境设定和改动规则，如果这个规则刚好和升级到的规则发生冲突，用户就该郁闷了，而且如果两条规则冲突了，防火墙该听谁的，会不会出现防火墙停止正常运行的情况，也许就因为考虑到这些因素，至今我没见过有多少个产品会提供过滤规则更新功能的，这并不能和杀毒软件的病毒特征库升级原理相提并论。

为了解决这种鱼与熊掌的问题，人们对包过滤技术进行了改进，这种改进后的技术称为“动态包过滤”（市场上存在一种“基于状态的包过滤防火墙”技术，即 stateful-based packet filtering，它们其实是同一类型），与它的前辈相比，动态包过滤功能在保持着原有静态包过滤技术和过滤规则的基础上，会对已经成功与计算机连接的报文传输进行跟踪，并且判断该连接发送的数据包是否会对系统构成威胁，一旦触发其判断机制，防火墙就会自动产生新的临时过滤规则或者把已经存在的过滤规则进行修改，从而阻止该有害数据的继续传输，但是由于动态包过滤需要消耗额外的资源和时间来提取数据包内容进行判断处理，所以与静态包过滤相比，它会降低运行效率，但是静态包过滤已经几乎退出市场了，我们能选择的，大部分也只有动态包过滤防火墙了。

基于包过滤技术的防火墙，其缺点是很显著的：它得以进行正常工作的一切依据都在于过滤规则的实施，但是偏又不能满足建立精细规则的要求（规则数量和防火墙性能成反比），而且它只能工作于网络层和传输层，并不能判断高级协议里的数据是否有害，但是由于它廉价，容易实现，所以它依然服役在各种领域，在技术人员频繁的设置下为我们工作着。

2．应用代理技术

由于包过滤技术无法提供完善的数据保护措施，而且一些特殊的报文攻击仅仅使用过滤的方法并不能消除危害（如 syn 攻击、icmp 洪水等），因此人们需要一种更全面的防火墙保护技术，在这样的需求背景下，采用“应用代理”技术的防火墙诞生了。代理服务器作为一个为用户保密或者突破访问限制的数据转发通道，在网络上广泛应用。一个完整的代理设备包含一个服务端和客户端，服务端接收来自用户的请求，调用自身的客户端模拟一个基于用户请求的连接到目标服务器，再把目标服务器返回的数据转发给用户，完成一次代理工作过程。那么，如果在一台代理设备的服务端和客户端之间连接一个过滤措施，这样的思想便造就了“应用代理”防火墙，这种防火墙实际上就是一台小型的带有数据检测过滤功能的透明代理服务器，但是它并不是单纯地在一个代理设备中嵌入包过滤技术，

而是一种被称为“应用协议分析”的新技术。

“应用协议分析”技术工作在OSI模型的最高层——应用层上，在这一层里能接触到的所有数据都是最终形式，也就是说，防火墙“看到”的数据和我们看到的是一样的，而不是一个个带着地址端口协议等原始内容的数据包，因而它可以实现更高级的数据检测过程。整个代理防火墙把自身映射为一条透明线路，在用户方面和外界线路看来，它们之间的连接并没有任何阻碍，但是这个连接的数据收发实际上是经过了代理防火墙转向的，当外界数据进入代理防火墙的客户端时，“应用协议分析”模块便根据应用层协议处理这个数据，通过预置的处理规则（没错，又是规则，防火墙离不开规则）查询这个数据是否带有危害，由于这一层面对的已经不再只是组合有限的报文协议，甚至可以识别类似于“get /sql.asp?id=1 and 1”的数据内容，所以防火墙不仅能根据数据层提供的信息判断数据，更能像管理员分析服务器日志那样“看”内容辨危害。而且由于工作在应用层，防火墙还可以实现双向限制，在过滤外部网络有害数据的同时也监控着内部网络的信息，管理员可以配置防火墙实现一个身份验证和连接时限的功能，进一步防止内部网络信息泄露的隐患。

最后，由于代理防火墙采取的是代理机制进行工作，内外部网络之间的通信都需先经过代理服务器审核，通过后再由代理服务器连接，根本没有给分隔在内外部网络两边的计算机直接会话的机会，可以避免入侵者使用“数据驱动”攻击方式（一种能通过包过滤技术防火墙规则的数据报文，但是当它进入计算机处理后，却变成能够修改系统设置和用户数据的恶意代码）渗透内部网络，可以说，“应用代理”是比包过滤技术更完善的防火墙技术。

但是，似乎任何东西都不可能逃避“墨菲定律”的规则，代理型防火墙的结构特征偏偏正是它的最大缺点，由于它是基于代理技术的，通过防火墙的每个连接都必须建立在为之创建的代理程序进程上，而代理进程自身是要消耗一定时间的，更何况代理进程里还有一套复杂的协议分析机制在同时工作，于是数据在通过代理防火墙时就不可避免地发生数据迟滞现象，换个形象的说法，每个数据连接在经过代理防火墙时都会先被“请进保安室喝杯茶搜搜身”再继续赶路，而“保安”的工作速度并不能很快。代理防火墙是以牺牲速度为代价换取了比包过滤防火墙更高的安全性能，在网络吞吐量不是很大的情况下，也许用户不会察觉到什么，然而到了数据交换频繁的时刻，代理防火墙就成了整个网络的瓶颈，而且一旦防火墙的硬件配置支撑不住高强度的数据流量而发生罢工，整个网络可能就会因此瘫痪了。所以，代理防火墙的普及范围还远远不及包过滤型防火墙，而在软件防火墙方面更是几乎没见过类似产品了——单机并不具备代理技术所需的条件，所以就目前整个庞大的软件防火墙市场来说，代理防火墙很难有立足之地。

3．状态监视技术

这是继“包过滤”技术和“应用代理”技术后发展的防火墙技术，它是checkpoint技术公司在基于“包过滤”原理的“动态包过滤”技术发展而来的，与之类似的有其他厂商联合发展的“深度包检测”（deep packet inspection）技术。这种防火墙技术通过一种被称为“状态监视”的模块，在不影响网络安全正常工作的前提下采用抽取相关数据的方法对网络通信的各个层次实行监测，并根据各种过滤规则作出安全决策。

“状态监视”（Stateful Inspection）技术在保留了对每个数据包的头部、协议、地址、端口、类型等信息进行分析的基础上，进一步发展了“会话过滤”（Session Filtering）功

能，在每个连接建立时，防火墙会为这个连接构造一个会话状态，里面包含了这个连接数据包的所有信息，以后这个连接都基于这个状态信息进行，这种检测的高明之处是能对每个数据包的内容进行监视，一旦建立了一个会话状态，则此后的数据传输都要以此会话状态作为依据，例如一个连接的数据包源端口是 8000，那么在以后的数据传输过程里防火墙都会审核这个包的源端口还是不是 8000，否则这个数据包就被拦截，而且会话状态的保留是有时间限制的，在超时的范围内如果没有再进行数据传输，这个会话状态就会被丢弃。状态监视可以对包内容进行分析，从而摆脱了传统防火墙仅局限于几个包头部信息的检测弱点，而且这种防火墙不必开放过多端口，进一步杜绝了可能因为开放端口过多而带来的安全隐患。

由于状态监视技术相当于结合了包过滤技术和应用代理技术，因此是最先进的，但是由于实现技术复杂，在实际应用中还不能做到真正的完全有效的数据安全检测，而且在一般的计算机硬件系统上很难设计出基于此技术的完善防御措施。

4.1.4　防火墙体系结构及组合形式

目前，防火墙的体系结构一般有以下几种：屏蔽路由器，双重宿主主机体系结构，被屏蔽主机体系结构和被屏蔽子网体系结构。

1．屏蔽路由器

这是防火墙最基本的构件。它可以由厂家专门生产的路由器实现，也可以用主机来实现。屏蔽路由器作为内外连接的唯一通道，要求所有的报文都必须在此通过检查。路由器上可以装基于 IP 层的报文过滤软件，实现报文过滤功能。许多路由器本身带有报文过滤配置选项，但一般比较简单。

单纯由屏蔽路由器构成的防火墙的危险带包括路由器本身及路由器允许访问的主机。它的缺点是一旦被攻陷后很难发现，而且不能识别不同的用户。

2．双穴主机网关

双穴主机网关是围绕具有双重宿主的主机计算机而构筑的，该计算机至少有两个网络接口。这样的主机可以充当与这些接口相连的网络之间的路由器；它能够从一个网络到另一个网络发送 IP 数据包。然而，实现双穴主机网关的防火墙体系结构禁止这种发送功能。因而，IP 数据包从一个网络（例如外部网）并不是直接发送到其他网络（例如内部的被保护的网络）。防火墙内部的系统能与双穴主机网关通信，同时防火墙外部的系统能与双穴主机网关通信，但是这些系统不能直接互相通信。它们之间的 IP 通信被完全阻止。

双穴主机网关的防火墙体系结构是相当简单的：双穴主机网关位于两者之间，并且被连接到外部网和内部网。如图 4-1 所示。

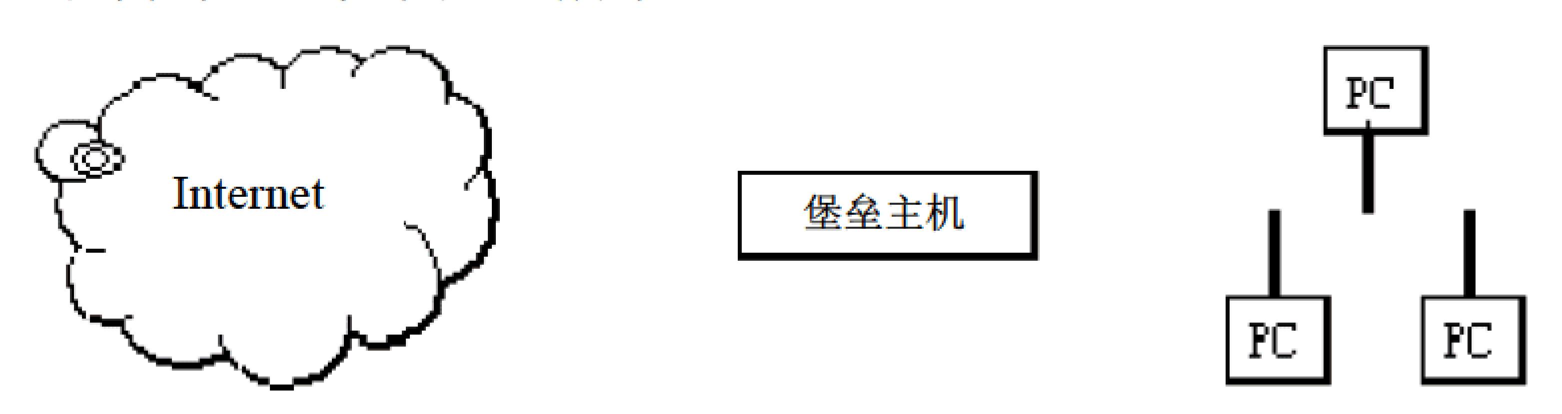


图 4-1　双重宿主主机体系结构

双穴主机网关优于屏蔽路由器的地方是：堡垒主机的系统软件可用于维护系统日志、

硬件复制日志或远程日志。这对于日后的检查很有用，但这不能帮助网络管理者确认内网中哪些主机可能已被黑客入侵。

双穴主机网关的一个致命弱点是：一旦入侵者侵入堡垒主机并使其只具有路由功能，则任何网上用户均可以随便访问内网。

3．被屏蔽主机网关

双穴主机网关体系结构提供来自与多个网络相连的主机的服务(但是路由关闭)，而被屏蔽主机网关体系结构使用一个单独的路由器提供来自仅仅与内部的网络相连的主机的服务。如图 4-2 所示。在这种体系结构中，主要的安全由数据包过滤提供（例如，数据包过滤用于防止人们绕过代理服务器直接相连）。

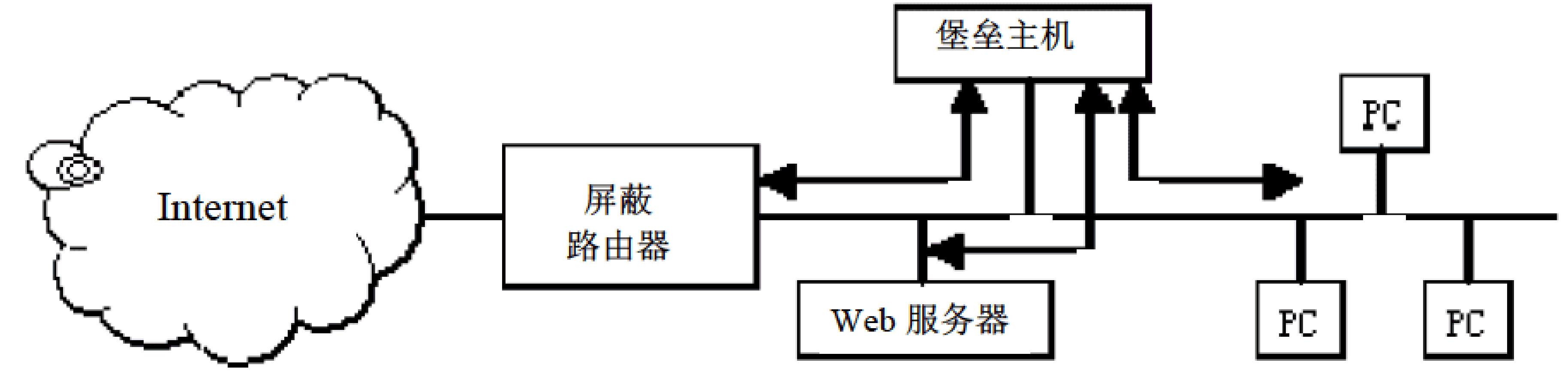


图 4-2　单地址堡垒主机

在屏蔽的路由器上的数据包过滤是按这样一种方法设置的：即堡垒主机是 Internet 上的主机能连接到内部网络上的系统的桥梁（例如，传送进来的电子邮件）。即使这样，也仅有某些确定类型的连接被允许。任何外部的系统试图访问内部的系统或者服务将必须连接到这台堡垒主机上。因此，堡垒主机需要拥有高等级的安全。

数据包过滤也允许堡垒主机开放可允许的连接（什么是“可允许”将由用户的站点的安全策略决定）到外部世界。

在屏蔽的路由器中数据包过滤配置可以按下列之一执行。

（1）允许其他的内部主机为了某些服务与 Internet 上的主机连接（即允许那些已经由数据包过滤的服务）。

（2）不允许来自内部主机的所有连接（强迫那些主机经由堡垒主机使用代理服务）。

用户可以针对不同的服务混合使用这些手段；某些服务可以被允许直接经由数据包过滤，而其他服务可以被允许仅仅间接地经过代理。这完全取决于用户实行的安全策略。

因为这种体系结构允许数据包从 Internet 向内部网的移动，所以，它的设计比没有外部数据包能到达内部网络的双穴主机网关体系结构似乎是更冒风险。实际上双穴主机网关体系结构在防备数据包从外部网络穿过内部的网络也容易产生失败。进而言之，保卫路由器比保卫主机较易实现，因为它提供非常有限的服务组。多数情况下，被屏蔽主机网关体系结构提供比双穴主机网关体系结构具有更好的安全性和可用性。

4．被屏蔽子网

屏蔽子网体系结构通过添加额外的安全层到被屏蔽主机体系结构，即通过添加周边网络更进一步地把内部网络与 Internet 隔离开。如图 4-3 所示，在这种结构下，即使攻破了堡垒主机，也不能直接侵入内部网络（他将必须通过内部路由器）。

堡垒主机是用户的网络上最容易受侵袭的机器。任凭用户尽最大的力气去保护它，它仍是最有可能被侵袭的机器，因为它本质上是能够被侵袭的机器。如果在屏蔽主机体系结构中，用户的内部网络对来自用户的堡垒主机的侵袭门户洞开，那么用户的堡垒主机是非

常诱人的攻击目标。在它与用户的其他内部机器之间没有其他的防御手段时（除了它们可能有的主机安全之外，这通常是非常少的）。如果有人成功地侵入屏蔽主机体系结构中的堡垒主机，那就毫无阻挡地进入了内部系统。

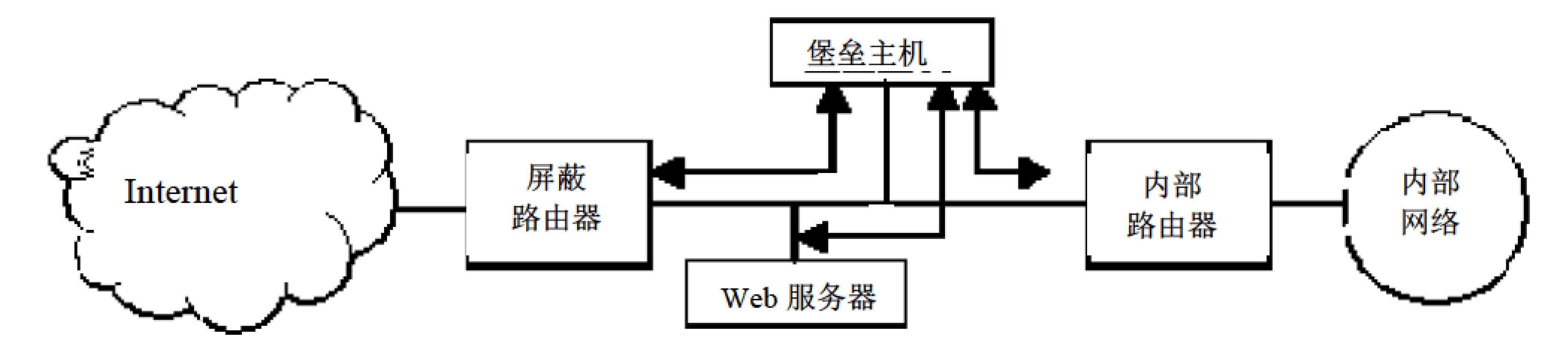


图 4-3　屏蔽子网体系结构

通过在周边网络上隔离堡垒主机，能减少在堡垒主机上侵入的影响。可以说，它只给入侵者一些访问的机会，但不是全部。屏蔽子网体系结构的最简单的形式为，两个屏蔽路由器，每一个都连接到周边网。一个位于周边网与内部网络之间，另一个位于周边网与外部网络之间（通常为 Internet）。为了侵入用这种类型的体系结构构筑的内部网络，侵袭者必须要通过两个路由器。即使侵袭者设法侵入堡垒主机，他将仍然必须通过内部路由器。在此情况下，没有损害内部网络的单一的易受侵袭点。作为入侵者，只是进行了一次访问。

1）周边网络

周边网络是另一个安全层，是在外部网络与用户的被保护的内部网络之间的附加的网络。如果侵袭者成功地侵入用户的防火墙的外层领域，周边网络在那个侵袭者与用户的内部系统之间提供一个附加的保护层。

在许多网络结构中，用给定网络上的任何机器来查看这个网络上的每一台机器的通信是可能的，如以太网、令牌环和 FDDI。探听者可以监听 Telnet、FTP 以及 rlogin 会话期间使用过的口令，偷看敏感信息等；探听者能完全监视何人在使用网络。

对于周边网络，如果攻击者侵入周边网络上的堡垒主机，他也仅能探听到周边网上的通信，内部网络的通信仍是安全的。

2）堡垒主机

在屏蔽的子网体系结构中，用户把堡垒主机连接到周边网；这台主机便是接受来自外界连接的主要入口。例如：对于进来的电子邮件（SMTP）会话，传送电子邮件到站点；对于进来的 FTP 连接，转接到站点的匿名 FTP 服务器；对于进来的域名服务（DNS）站点查询等等。

从内部的客户端到在 Internet 上的服务器的出站服务按如下任一方法处理：在外部和内部的路由器上设置数据包过滤来允许内部的客户端直接访问外部的服务器；设置代理服务器在堡垒主机上运行来允许内部的客户端间接地访问外部的服务器。用户也可以设置数据包过滤来允许内部的客户端在堡垒主机上同代理服务器交谈，反之亦然。但是禁止内部的客户端与外部世界之间直接通信（即拨号入网方式）。

3）内部路由器

内部路由器有时被称为阻塞路由器，它保护内部的网络使之免受 Internet 和周边网的侵犯。

内部路由器为用户的防火墙执行大部分的数据包过滤工作。它允许从内部网到 Internet

的有选择的出站服务。

内部路由器所允许的在堡垒主机和用户的内部网之间服务可以不同于内部路由器所允许的在 Internet 和用户的内部网之间的服务。限制堡垒主机和内部网之间服务的理由是减少了堡垒主机被攻破时对内部网的危害。

4）外部路由器

外部路由器有时被称为访问路由器，保护周边网和内部网使之免受来自 Internet 的侵犯。实际上，外部路由器倾向于允许几乎任何东西从周边网出站，并且它们通常只执行非常少的数据包过滤。保护内部机器的数据包过滤规则在内部路由器和外部路由器上基本上应该是一样的；如果在规则中有允许侵袭者访问的错误，错误就可能出现在两个路由器上。

一般，外部路由器由外部群组提供（例如用户的 Internet 供应商），同时用户对它的访问被限制。外部群组可能愿意放入一些通用型数据包过滤规则来维护路由器，但是不愿意使用维护复杂或者频繁变化的规则组。

外部路由器能有效地执行的安全任务之一是：阻止从 Internet 上伪造源地址进来的任何数据包。这样的数据包自称来自内部的网络，但实际上是来自 Internet。

5．防火墙的组合形式

建造防火墙时，一般很少采用单一的技术，通常是多种解决不同问题的技术的组合。这种组合主要取决于网管中心向用户提供什么样的服务，以及网管中心能接受什么等级风险。采用哪种技术主要取决于经费，投资的大小或技术人员的技术、时间等因素。一般有以下几种形式：

- 使用多堡垒主机；
- 合并内部路由器与外部路由器；
- 合并堡垒主机与外部路由器；
- 合并堡垒主机与内部路由器；
- 使用多台内部路由器；
- 使用多台外部路由器；
- 使用多个周边网络；
- 使用双重宿主主机与屏蔽子网。

通常建立防火墙的目的在于保护内部网免受外部网的侵扰，但内部网络中每个用户所需要的服务和信息经常是不一样的，它们对安全保障的要求也不一样。例如，财务部分与其他部分分开，人事档案部分与办公管理分开等。还需要对内部网的部分站点再加以保护以免受内部的其他站点的侵袭，即在同一结构的两个部分之间，或者在同一内部网的两个不同组织结构之间再建立防火墙，也就是内部防火墙。许多用于建立外部防火墙的工具与技术也可用于建立内部防火墙。

4.2 用协议分析工具学习 TCP/IP

TCP/IP 协议是网络通信的基础，而防火墙又是网络安全的基础，了解 TCP/IP 协议是了解防火墙的工作原理和配置方法的基础，只有对 TCP/IP 协议有了基本的了解，才能理解

防火墙的工作原理以及配置理由。

下面通过一个试验来了解 TCP/IP 协议的相关知识，利用协议分析工具学习 TCP/IP，在学习的过程中能直观地看到数据的具体传输过程。

4.2.1　试验环境

进行本试验需要合适的网络环境以及对应的工具，具体包括两台安装 Windows 2000 计算机以及协议分析工具 IRIS。

1．网络环境

网络环境要求这两台计算机能够互相连接在一个网络环境中，如图 4-4 所示 。

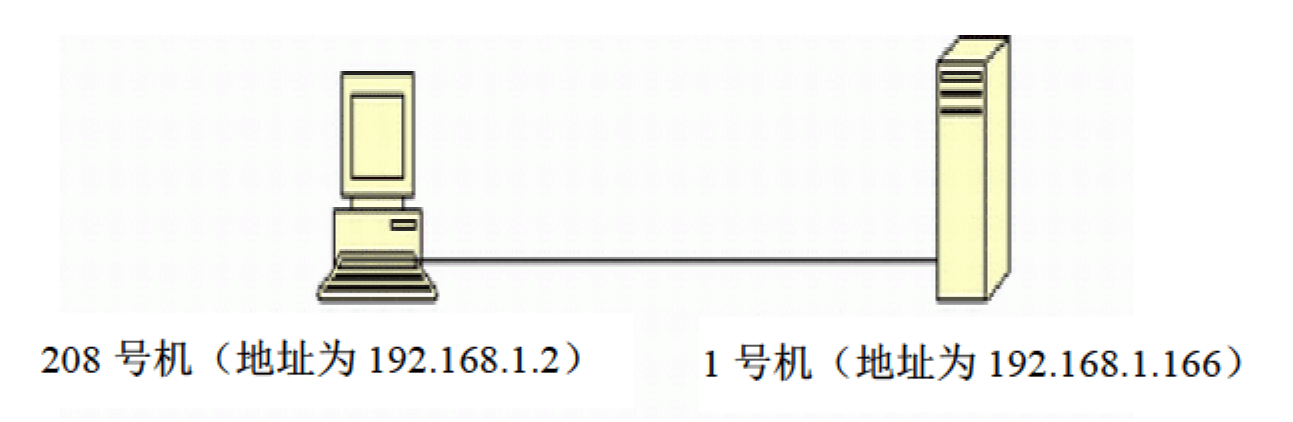


图 4-4　网络示意图

为了表述方便，用客户机代表地址为 192.168.1.2 的计算机，用服务器代表地址为 192.168.1.166 的计算机。

2．操作系统

两台机器都为 Windows 2000 ，在服务器上安装 FTP 服务。

3．协议分析工具

在客户机安装 TCP/IP 协议分析工具 IRIS 软件。

4.2.2　测试过程

1．测试例子

将服务器计算机中的一个文件通过 FTP 下载到客户机中。

2．IRIS 的设置

使用 IRIS 做 TCP/IP 协议分析以前需要对软件做适当的配置，具体步骤如下。

（1）软件安装完成后第一次运行，会出现 Setting 窗口，如图 4-5 所示。

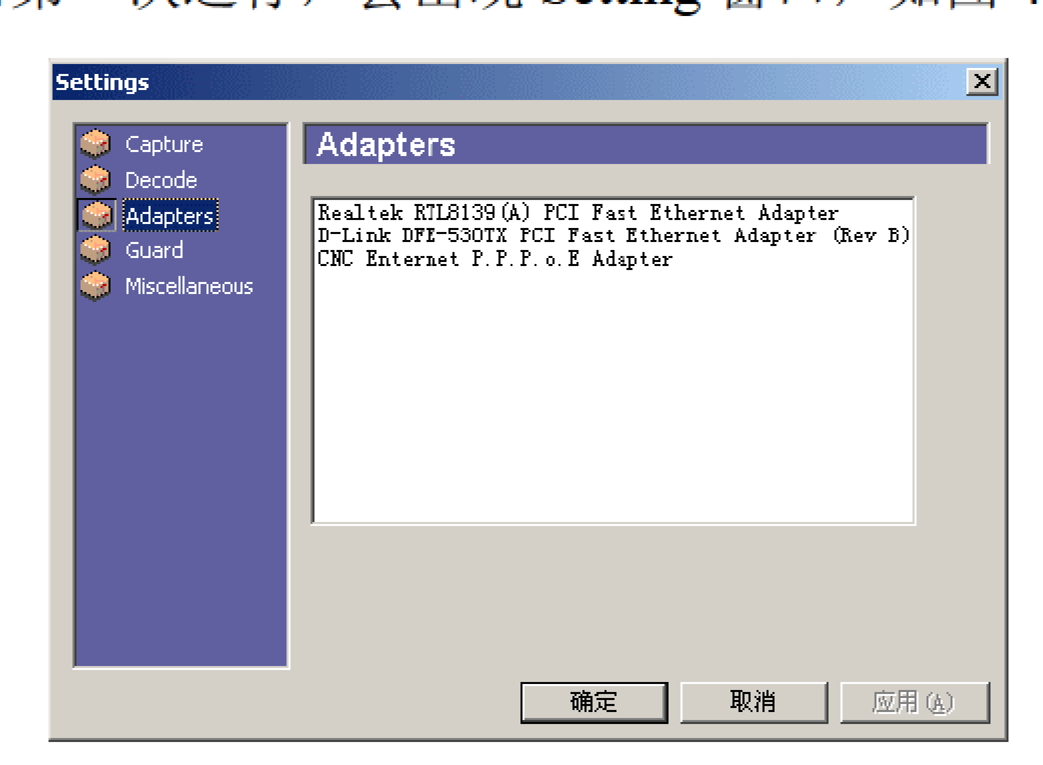


图 4-5　网卡设置窗口

（2）选择窗口左边列表中的 Adapters，然后在右边窗口中选择需要监控的网卡，然后单击“确定”按钮，出现 IRIS 主窗口，如图 4-6 所示。

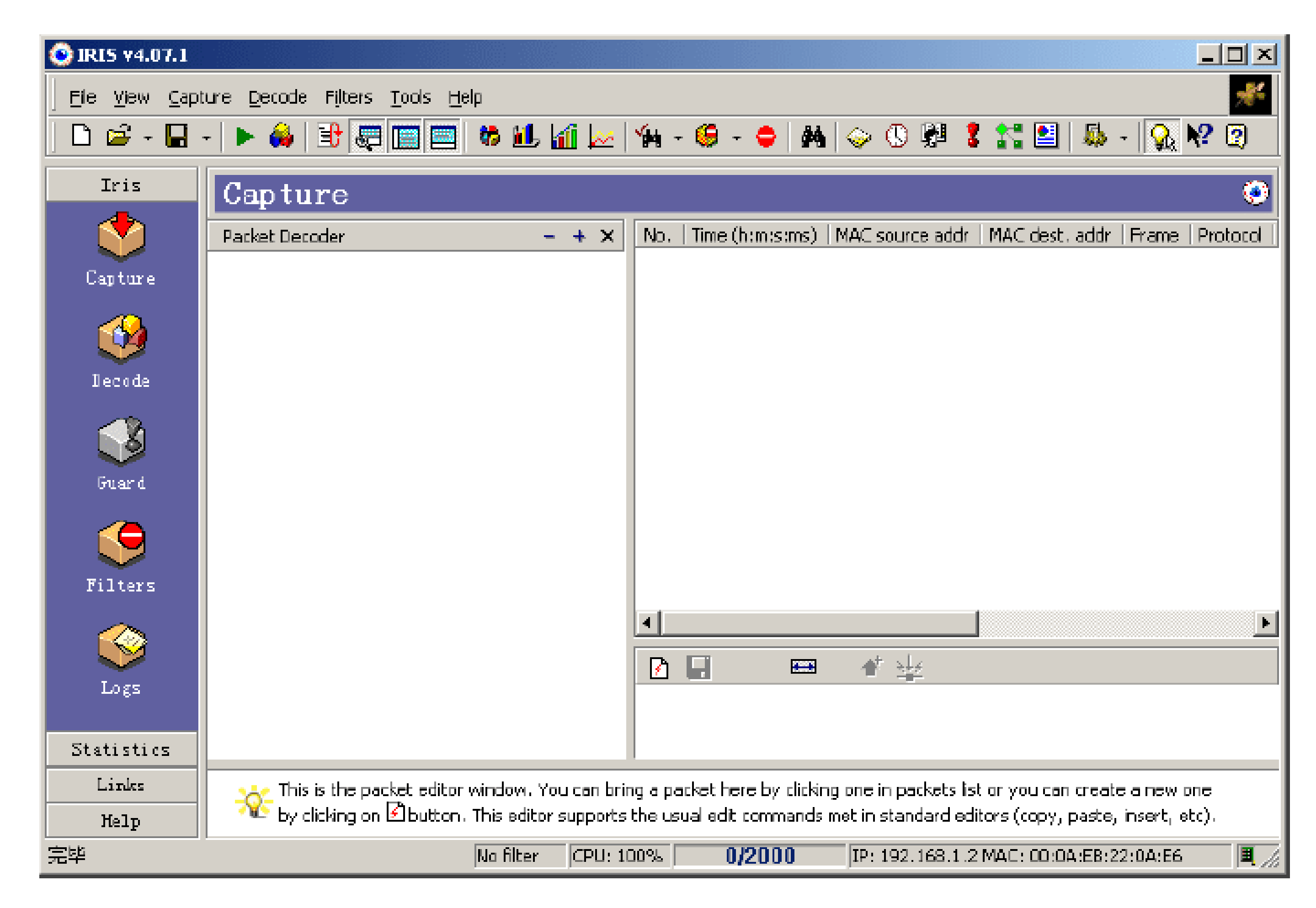
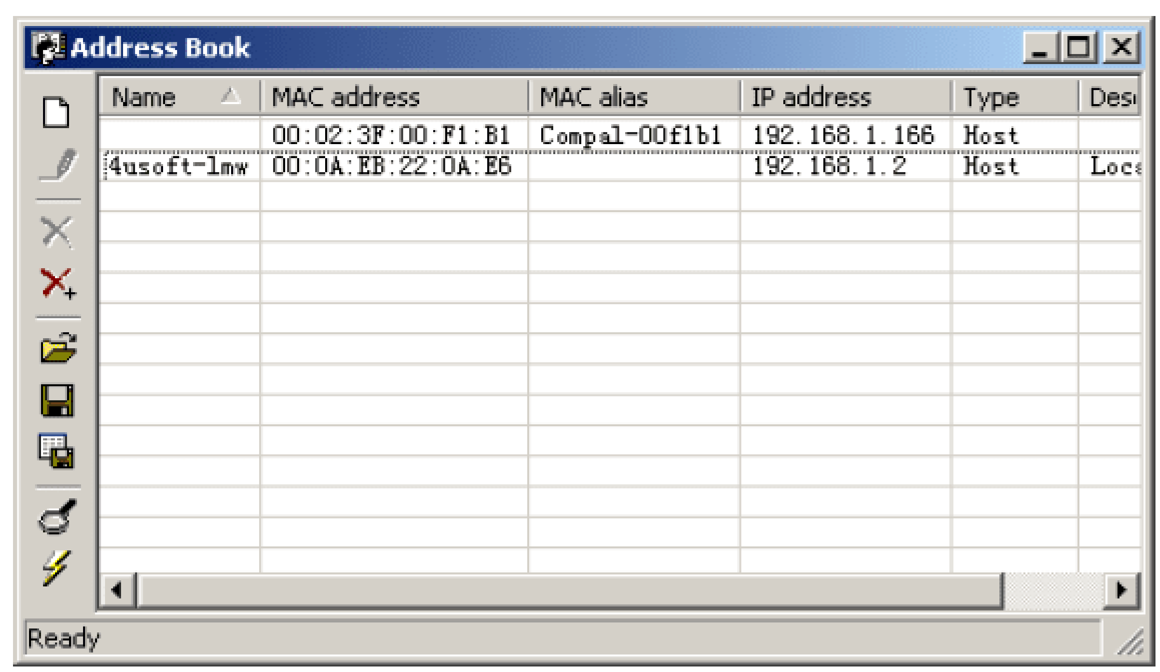


图 4-6 IRIS 主窗口

（3）按 Ctrl+B 键弹出 Address Book 对话框，如图 4-7 所示，在表中填写客户机和服务器的 IP 地址，或者单击窗口左边的 Discover Host 按钮，自动发现客户机和服务器的 IP 地址等信息。

（4）按 Ctrl+E 键弹出 Edit filter settings 对话框，选择窗口左边 IP address 项，从窗口右边的 IP address 框中找出客户机和服务器的 IP 地址，将它们拖到下面的列表框中，在选择客户端和服务器之间的数据包方向为双向，如图 4-8 所示。



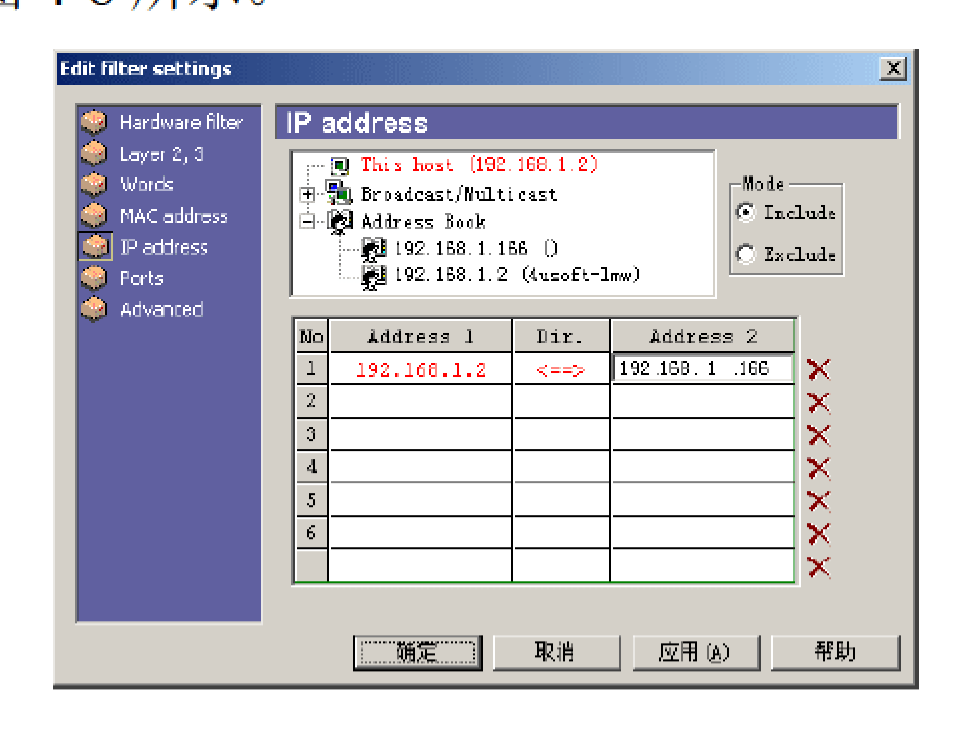


图 4-7 IP 地址表　　　　图 4-8 设置 IP 地址

3．抓包

抓取数据包的具体操作步骤如下。

（1）在 IRIS 的主窗口工具栏上，单击 Start/Stop capture 按钮。

（2）在浏览器的地址栏中输入 FTP://192.168.1.166，找到要下载的文件 Test.doc，如图 4-9 所示。

（3）右击该文件，在弹出的菜单中选择“复制到文件夹”命令，出现选择文件夹对话框，如图 4-10 所示，选择本地的一个目录，单击“确定”按钮开始下载。

（4）下载完后在 IRIS 工具栏中单击 Start/Stop capture 按钮，停止抓包，下载文件的整个过程中的数据包都被抓取下来，如图 4-11 所示。

提示： 为了能抓到 ARP 协议的包，在 Windows 2000 中运行 arp -d 清除 arp 缓存。

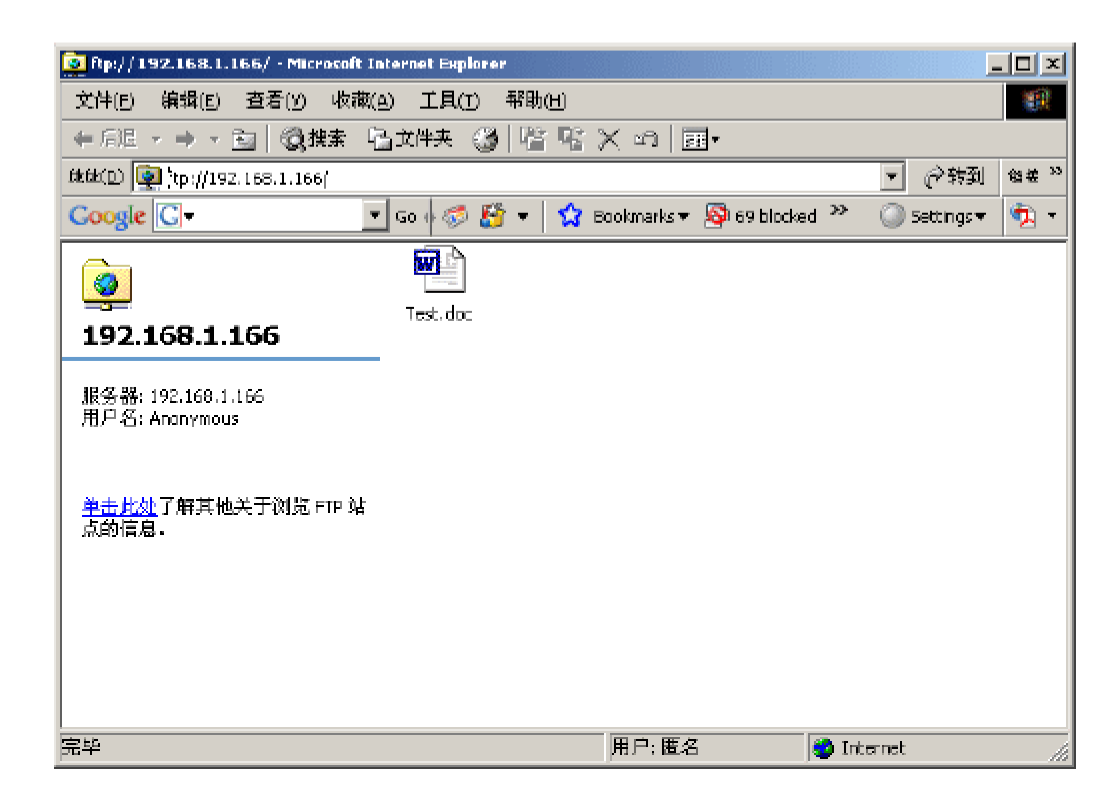




图 4-9　访问 Ftp 文件

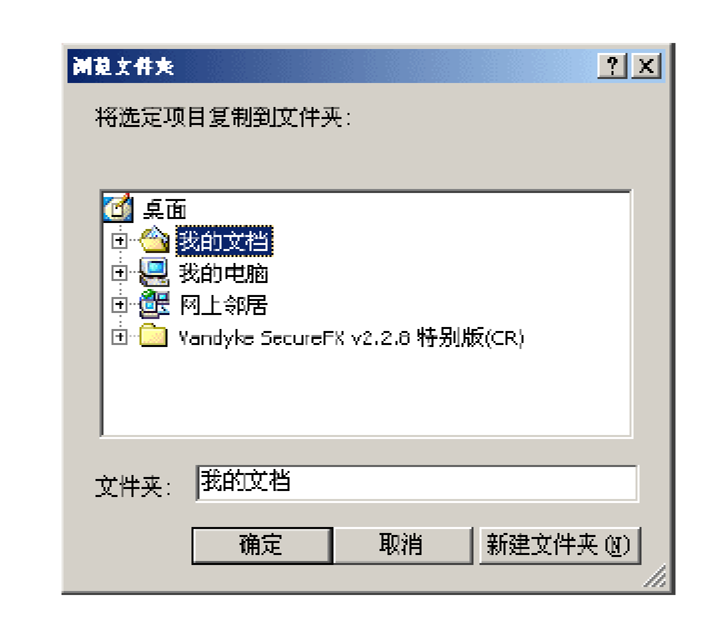


图 4-10　选择文件夹窗口

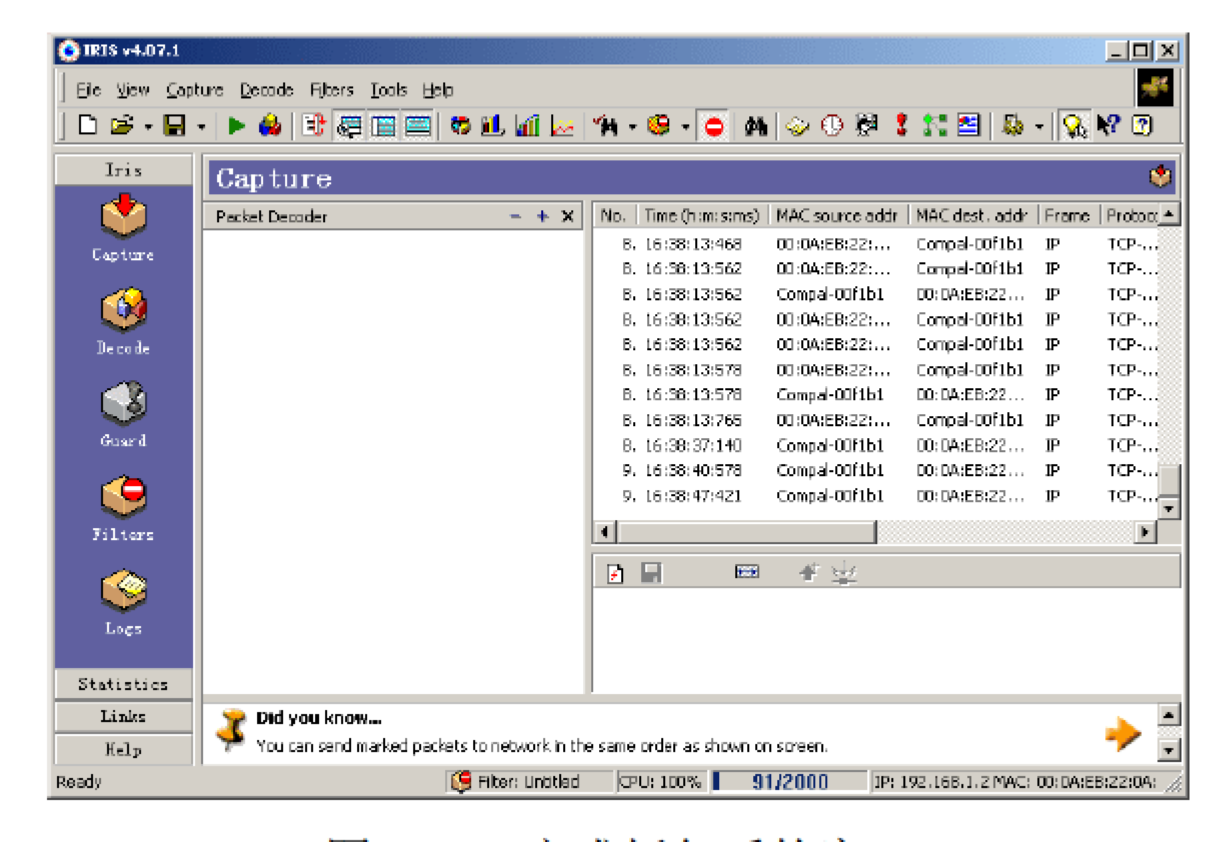


图 4-11　完成抓包后的窗口

4.2.3　过程分析

1．TCP/IP 的基本原理

为了能够对 TCP/IP 协议的理解，首先简要讲一下 TCP/IP 的基本原理。

（1）网络是分层的，每一层分别负责不同的通信功能。

TCP/IP 通常被认为是一个四层协议系统，TCP/IP 协议簇是一组不同的协议组合在一起构成的协议簇。尽管通常称该协议簇为 TCP/IP，但 TCP 和 IP 只是其中的两种协议而已，每一层负责不同的功能，如表 4-1 所示。

表 4-1　TCP/IP 的四层协议系统

TCP/IP 层描述	主要协议	主　要　功　能
应用层	HTTP、Telnet、FTP 和 E-mail 等	负责把数据传输到传输层或接收从传输层返回的数据
传输层	TCP 和 UPD	主要为两台主机上的应用程序提供端到端的通信，TCP 为两台主机提供可靠的数据通信。它所做的工作包括把应用程序交给它的数据分成合适的小块交给下面的网络层，确认接收到的分组，设置发送最后确认分组的超时时钟等。UPD 则为应用层提供一种非常简单的服务。它只是把称作数据报的分组从一台主机发送到另一台主机，但并不保证该数据能到达另一端

续表

TCP/IP 层描述	主要协议	主 要 功 能
网络层	ICMP、IP 和 IGMP	有时称作互联网层，主要为数据包选择路由，其中 IP 是 TCP/IP 协议簇中最为核心的协议。所有的 TCP、UPD、ICMP 及 IGMP 数据协议都以 IP 数据包格式传输
链路层	ARP、RARP 和设备驱动程序及接口卡	发送时将 IP 包作为帧发送；接收时把接收到的位组装成帧；提供链路管理、错误检测等

分层的概念说起来非常简单，但在实际的应用中非常的重要，在进行网络设置和排除故障时对网络层次理解得很透，将对工作有很大的帮助。例如：设置路由是网络层 IP 协议的事，要查找 MAC 地址是链路层 ARP 的事，常用的 Ping 命令由 ICMP 协议来做的。

各层协议的关系如图 4-12 所示，理解它们之间的关系对下面的协议分析非常重要。

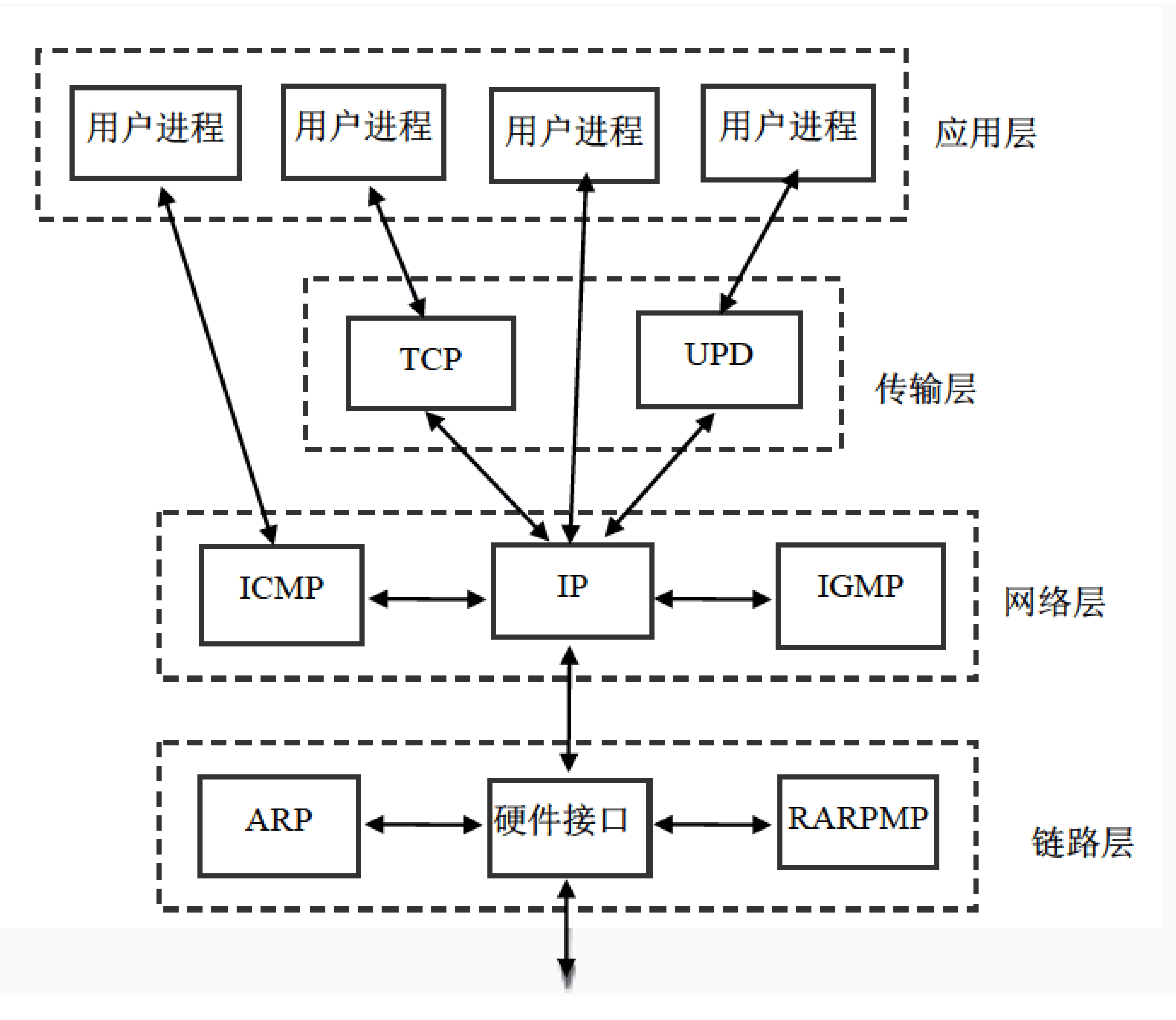


图 4-12　TCP/IP 协议簇

（2）数据发送时是自上而下，层层加码；数据接收时是自下而上，层层解码。

当应用程序用 TCP 传送数据时，数据被送入协议栈中，然后逐个通过每一层直到被当作一串比特流送入网络。其中每一层对收到的数据都要增加一些首部信息（有时还要增加尾部信息），该过程如图 4-13 所示。TCP 传给 IP 的数据单元称作 TCP 报文段或简称为 TCP 段。IP 传给网络接口层的数据单元称作 IP 数据报。通过以太网传输的比特流称作帧（Frame）。

数据发送时是按照图 4-13 自上而下，层层加码；数据接收时是自下而上，层层解码。

（3）逻辑上通信是在同级完成的。

垂直方向的结构层次是当今普遍认可的数据处理的功能流程。每一层都有与其相邻层的接口。为了通信，两个系统必须在各层之间传递数据、指令、地址等信息，通信的逻辑流程与真正的数据流的不同。虽然通信流程垂直通过各层次，但每一层都在逻辑上能够直

接与远程计算机系统的相应层直接通信。

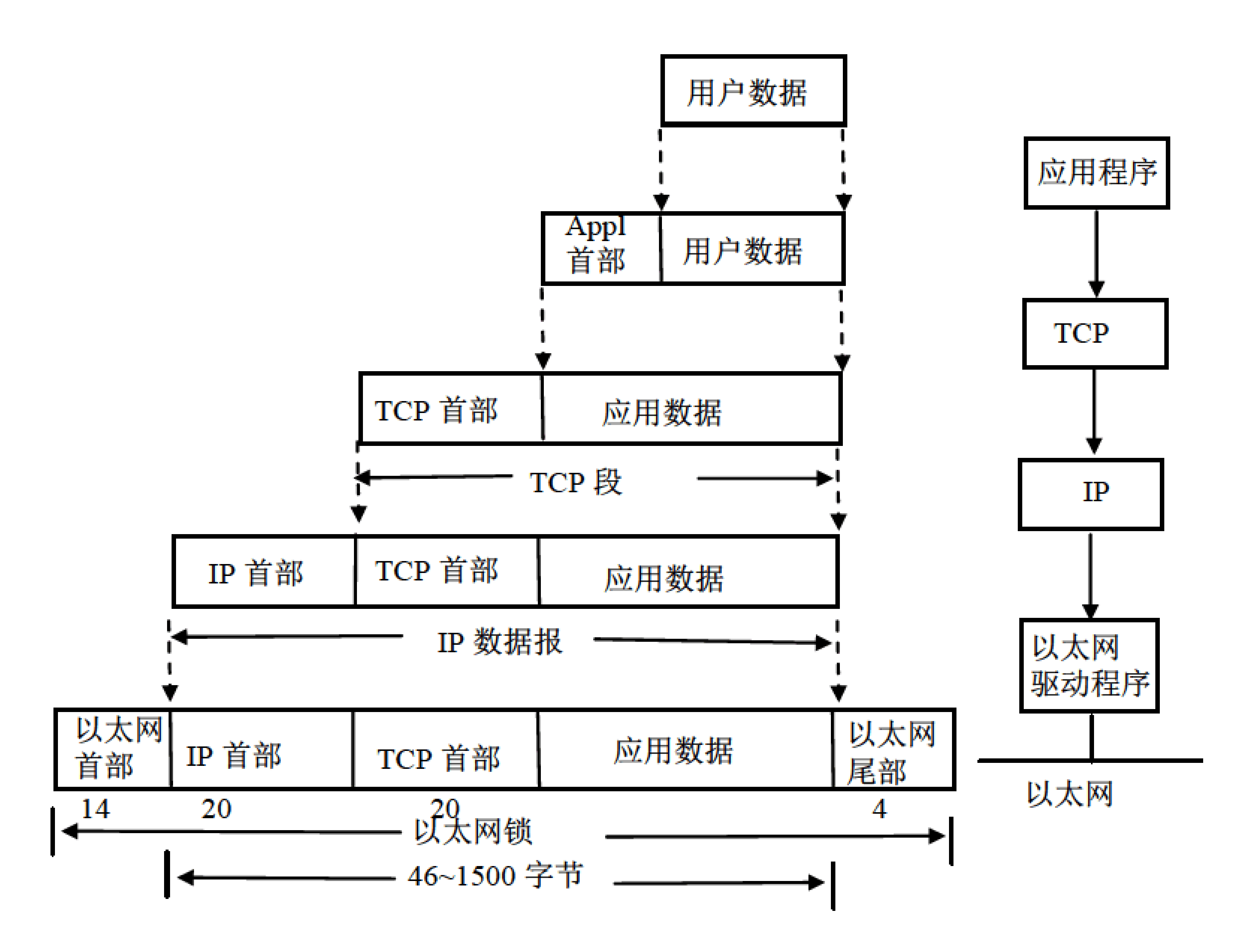


图 4-13　数据传输示意图

通信实际上是按垂直方向进行的，但在逻辑上通信是在同级进行的，如图 4-14 所示。

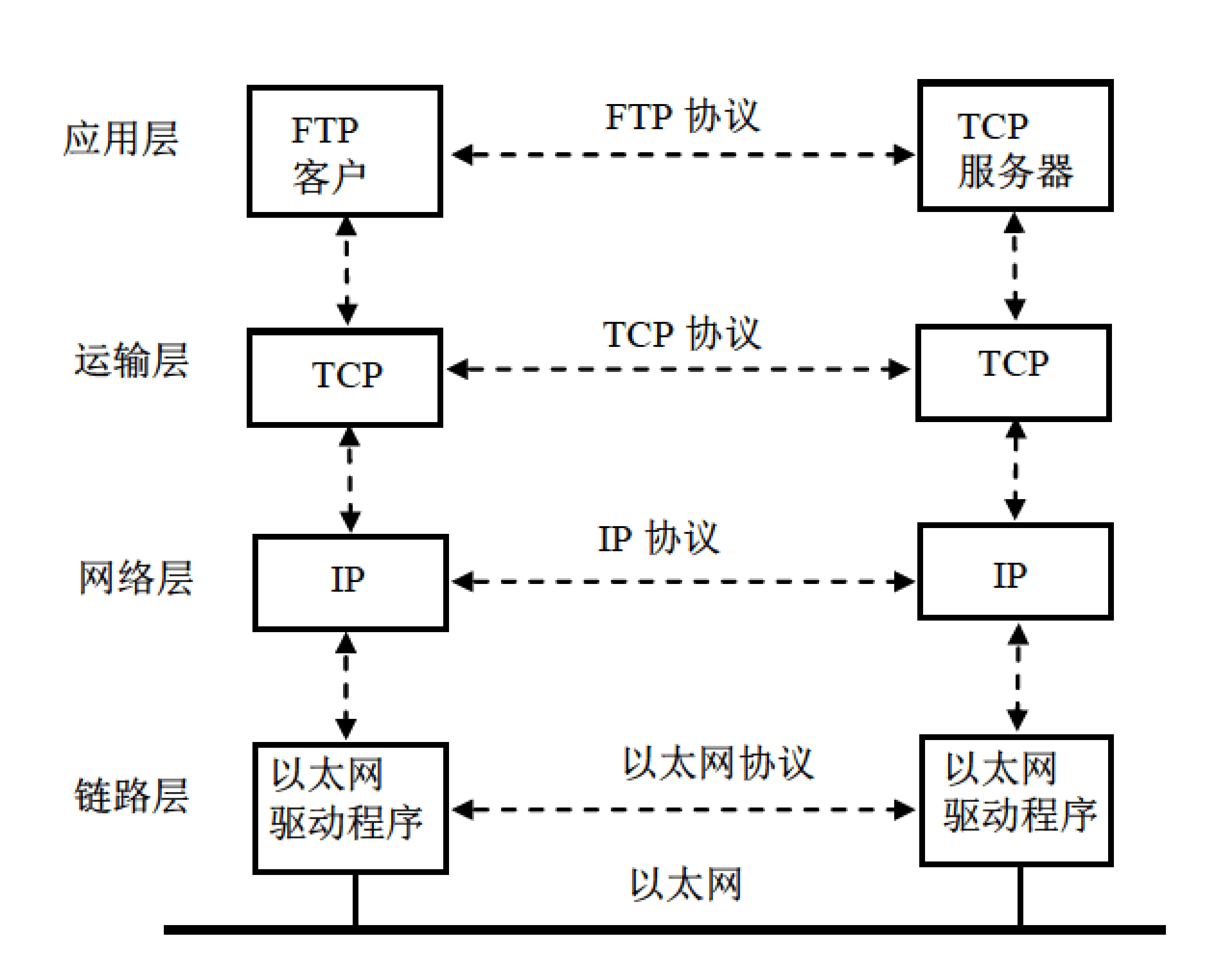


图 4-14　逻辑通信

2. 过程描述

为了更好地分析协议，先描述一下上述例子数据的传输步骤。如图 4-15 所示。

（1）FTP 客户端请求 TCP 用服务器的 IP 地址建立连接。

（2）TCP 发送一个连接请求分段到远端的主机，即用上述 IP 地址发送一份 IP 数据报。

（3）如果目的主机在本地网络上，那么 IP 数据报可以直接送到目的主机上。如果目的主机在一个远程网络上，那么就通过 IP 选路函数来确定位于本地网络上的下一站路由器地址，并让它转发 IP 数据报。在这两种情况下，IP 数据报都是被送到位于本地网络上的一台主机或路由器。

（4）本例是一个以太网，那么发送端主机必须把 32 位的 IP 地址变换成 48 位的以太网地址，该地址也称为 MAC 地址，它是出厂时写到网卡上的世界唯一的硬件地址。把 IP 地址翻译到对应的 MAC 地址是由 ARP 协议完成的。

（5）如图的虚线所示，ARP 发送一份称作 ARP 请求的以太网数据帧给以太网上的每个主机，这个过程称作广播。ARP 请求数据帧中包含目的主机的 IP 地址，其意思是“如果你是这个 IP 地址的拥有者，请回答你的硬件地址。”

（6）目的主机的 ARP 层收到这份广播后，识别出这是发送端在寻问它的 IP 地址，于是发送一个 ARP 应答。这个 ARP 应答包含 IP 地址及对应的硬件地址。

（7）收到 ARP 应答后，使 ARP 进行请求—应答交换的 IP 数据包现在就可以传送了。

（8）发送 IP 数据报到目的主机。

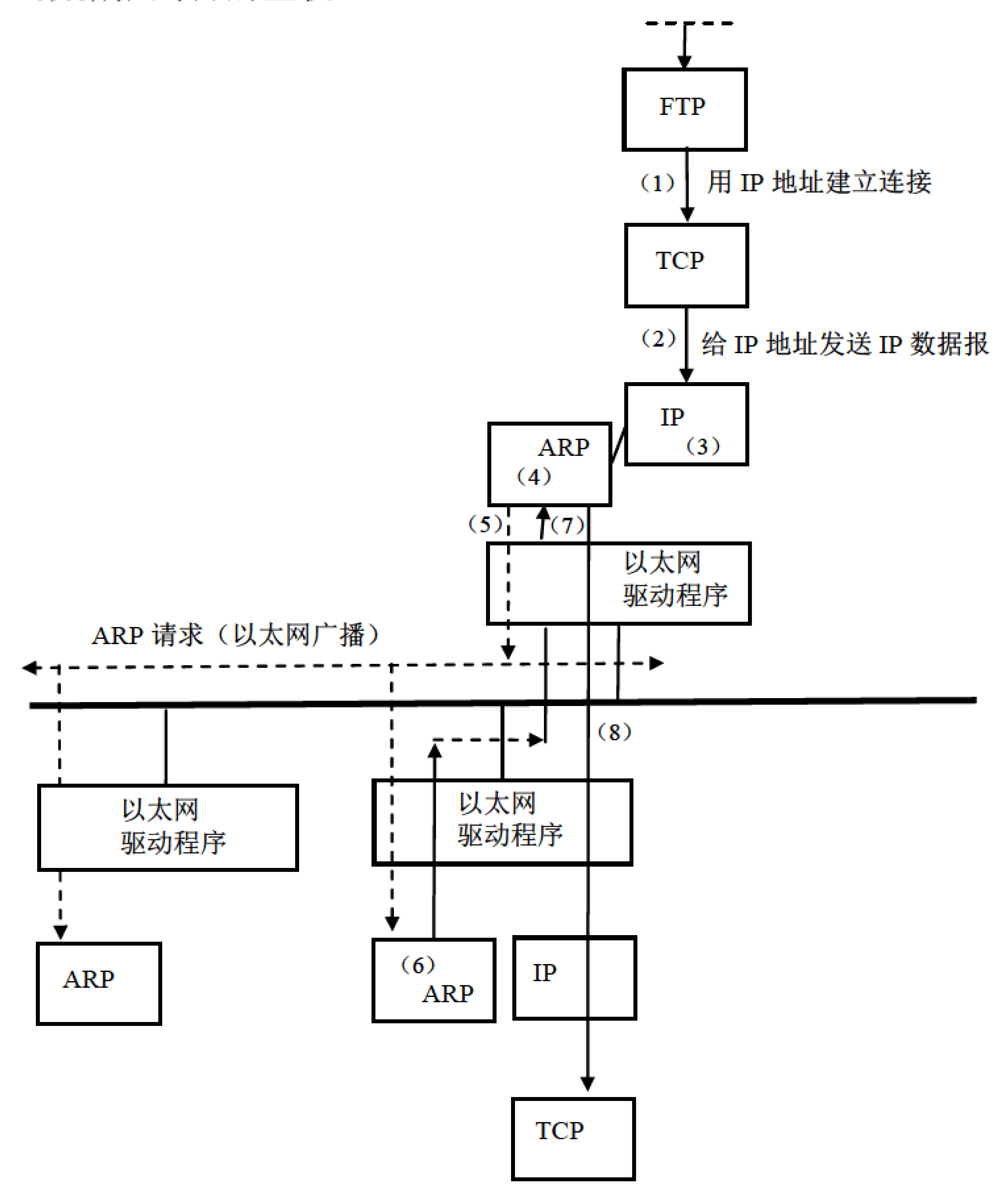


图 4-15 通信过程示意图

4.2.4 实例分析

下面通过分析用 iris 捕获的包来分析一下 TCP/IP 的工作过程，为了更清晰地解释数据传送的过程，我们按传输的不同阶段抓了四组数据，分别是查找服务器、建立连接、数据传输和终止连接。每组数据，按照显示数据包、解释该数据包、分析该包的头信息三步进行解释。

1. 查找服务器

（1）显示数据包

第三个和第四个数据包是 ARP 数据包，这两行数据就是查找服务器及服务器应答的过程，如图 4-16 所示。

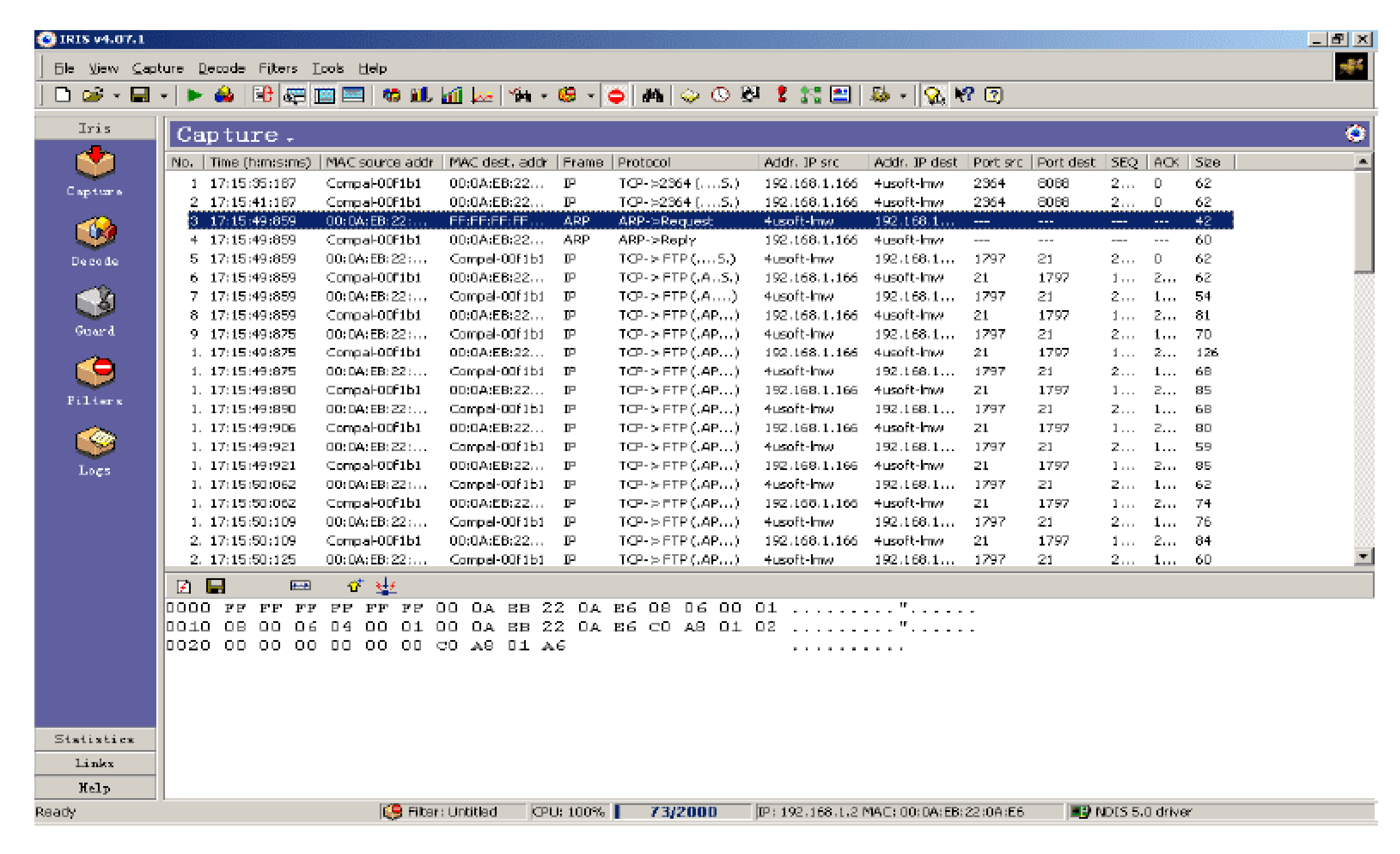


图 4-16　抓取的 ARP 包

（2）解释数据包

在第 3 行中，源端主机的 MAC 地址是 00:0A:EB:22:0A:E6。目的端主机的 MAC 地址是 FF:FF:FF:FF:FF:FF，这个地址是十六进制表示的，F 换算为二进制就是 1111，全 1 的地址就是广播地址。所谓广播就是向本网上的每台网络设备发送信息，电缆上的每个以太网接口都要接收这个数据帧并对它进行处理，这一行反映的是 4.2.3 节第 2 小节过程描述中步骤（5）的内容，ARP 发送一份称作 ARP 请求的以太网数据帧给以太网上的每个主机。网内的每个网卡都接到这样的信息"谁是 192.168.1.166 的 IP 地址的拥有者，请将你的硬件地址告诉我"。

第 4 行反映的是 4.2.3 节第 2 小节过程描述中步骤（6）的内容。在同一个以太网中的每台机器都会"接收"到这个报文，但正常状态下除了服务器外其他主机应该会忽略这个报文，而服务器的 ARP 层收到这份广播报文后，识别出这是发送端在寻问它的 IP 地址，于是发送一个 ARP 应答。告知自己的 IP 地址和 MAC 地址。第 4 行可以清楚地看出服务器回答的信息，其 MAC 地址 00:02:3F:00:F1:B1。

这两行反映的是数据链路层之间一问一答的通信过程。这个过程就像我要在一个坐满人的教室找一个叫"张三"的人，在门口喊了一声"张三"，这一声大家都听见了，这就叫广播。张三听到后有回应，别人听到了没有回应，这样就与张三取得了联系。

（3）头信息分析

选择第 5 个数据包，从窗口左边看到两个头信息：以太网（Ethernet）和 ARP，如图 4-17 所示。

以太网的头信息包括三个部分，目的 MAC 地址、源 MAC 地址和帧类型，如表 4-2 所示，括号内的数均为该字段所占字节数，以太网报头中的前两个字段是以太网的源地址和目的地址。目的地址为全 1 的特殊地址是广播地址。电缆上的所有以太网接口都要接收广

播的数据帧。两个字节长的以太网帧类型表示后面数据的类型。对于 ARP 请求或应答来说，该字段的值为 0806。

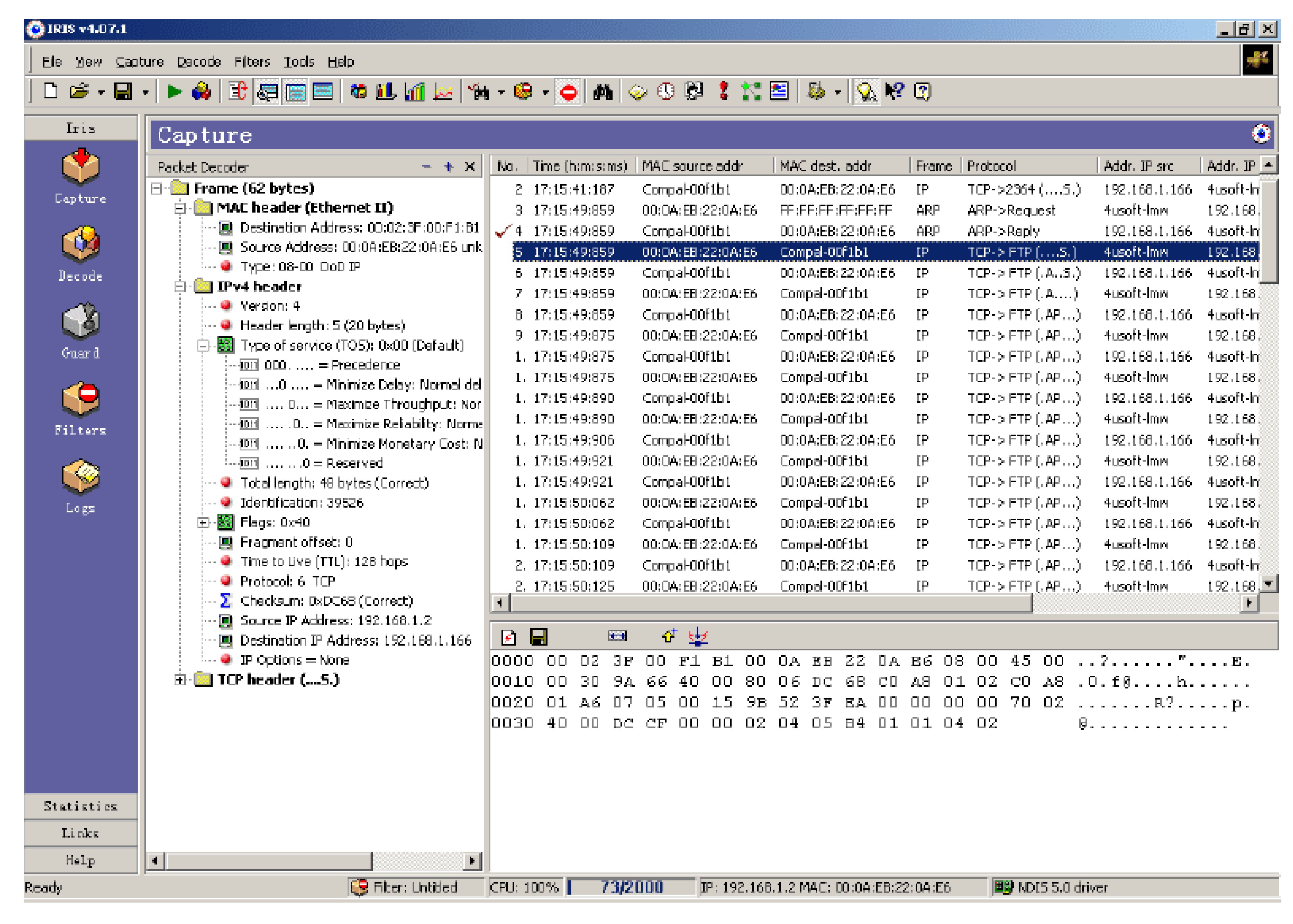


图 4-17　数据包头信息

第 2 行中可以看到，尽管 ARP 请求是广播的，但是 ARP 应答的目的地址却是服务器 MAC 地址（00:02:3F:00:F1:B1）。ARP 应答是直接送到请求端主机的，如表 4-2 所示。

表 4-2　ARP 应答

行	以太网目的地址（6）	以太网源地址（6）	帧类型（2）
1	FF:FF:FF:FF:FF:FF	00:0A:EB:22:0A:E6	08 06
2	00:0A:EB:22:0A:E6	00:02:3F:00:F1:B1	08 06

ARP 协议的头信息如表 4-3 所示，其中包括如下信息。

① 硬件类型字段表示硬件地址的类型，它的值为 1 即表示以太网地址。

② 协议类型字段表示要映射的协议地址类型。它的值为 0800 即表示 IP 地址。它的值与包含 IP 数据报的以太网数据帧中的类型字段的值相同。

③ 硬件地址长度和协议地址长度分别指出硬件地址和协议地址的长度，以字节为单位。对于以太网上 IP 地址的 ARP 请求或应答来说，它们的值分别为 6 和 4。

④ Op 即操作（Opoperation），1 是 ARP 请求、2 是 ARP 应答、3 是 RARP 请求和 4 为 RARP 应答，第 2 行中该字段值为 2 表示应答。

⑤ 发送端的硬件地址、发送端的 IP 地址、目的端的硬件地址和目的端 IP 地址。

> **提示：** 在以太网的数据帧报头中和 ARP 请求数据帧中都有发送端的硬件地址。对于一个 ARP 请求来说，除目的端硬件地址外的所有其他的字段都有填充值。

第 2 行为应答，当系统收到一份目的端为本机的 ARP 请求报文后，它就把硬件地址填进去，然后用目的端 IP 地址和 Mac 地址分别替换源 IP 地址和 Mac 地址，并把操作字段置为 2，最后把它发送回去。

表 4-3　ARP 帧头信息

行	硬件类型（2）	协议类型（2）	硬件地址长度（1）	协议地址长度（1）	Op（2）	源 Mac（6）	源 IP 地址（4）	目的 Mac（6）	目的 IP（4）
1	00 01	08 00	06	04	00 01	000AEB220AE6	C0A80102	000000000000	C0A801A6
2	00 01	08 00	06	04	00 02	00023F00F1B1	C0A801A6	000AEB220AE6	C0A80102

2．建立连接

（1）显示数据包

建立连接的过程是通过三个步骤来完成的，就是从第五个到第七个数据包，如图 4-18 所示。

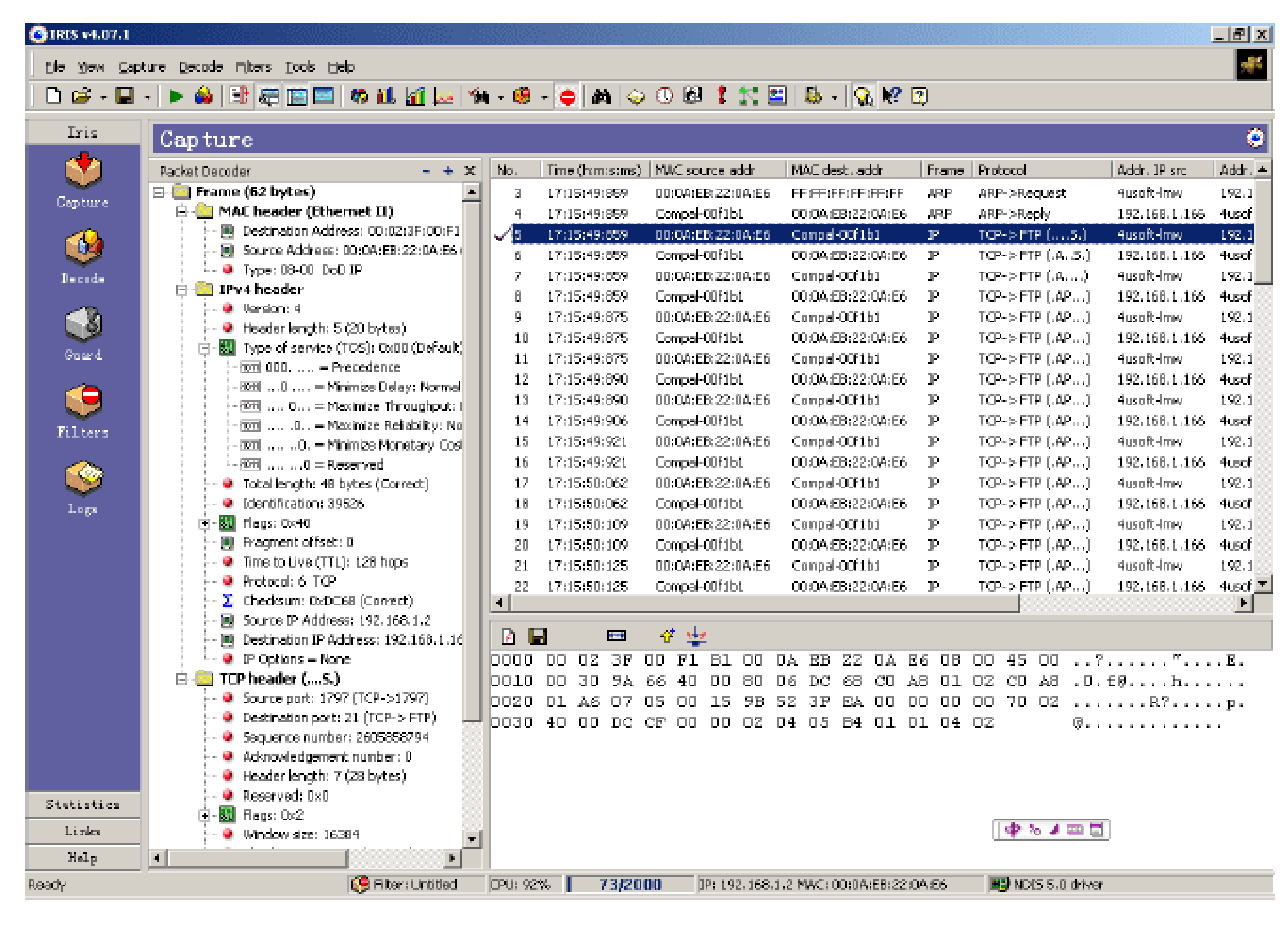


图 4-18　建立连接数据包

（2）解释数据包

这三行数据是两机建立连接的过程。

这三行的核心意思就是 TCP 协议的三次握手。TCP 的数据包是靠 IP 协议来传输的。但 IP 协议是只管把数据送出去，但不能保证 IP 数据报能成功地到达目的地，保证数据的可靠传输是靠 TCP 协议来完成的。当接收端收到来自发送端的信息时，接受端详细发送一条应答信息，意思是：“我已收到你的信息了。”第三组数据将能看到这个过程。TCP 是一个面向连接的协议。无论哪一方向另一方发送数据之前，都必须先在双方之间建立一条连接。建立连接的过程就是三次握手的过程。

这个过程就像我找张三向他借几本书，第一步：我说“你好，我是李四”，第二步：张三说“你好，我是张三”，第三步：我说“我找你借几本书”，这样通过问答就确认对方身份，建立了联系。

下面来分析一下此例的三次握手过程。

1）客户机发送一个初始序号（SEQ）为 2605858794 的数据包给服务器。

2）服务器收到这个序号后，将此序号加 1 值为 2605858795 作为应答信号（ACK），同时随机产生一个初始序号（SEQ）1341443022，这两个信号同时发回到客户机，意思为：“消息已收到，让我们的数据流以 1341443022 这个数开始。”

3）客户机收到后将确认序号设置为服务器的初始序号（SEQ）1341443022 加 1 为

1341443033 作为应答信号。

以上三步完成了三次握手，双方建立了一条通道，接下来就可以进行数据传输了。

（3）头信息分析

分析 TCP 头信息就可以看出，在握手过程中 TCP 头部的相关字段也发生了变化。如图 4-19 所示，第 5 数据包包含了三部分信息：以太网（Ethernet）、IP 和 TCP。

头信息少了 ARP 多了 IP、TCP，下面的过程也没有 ARP 的参与，可以这样理解，在局域网内，ARP 负责的是在众多联网的计算机中找到要找的计算机，找到工作就完成了。

以太网的头信息与第 3、4 行不同的是帧类型为 08 00，指明该帧类型为 IP。

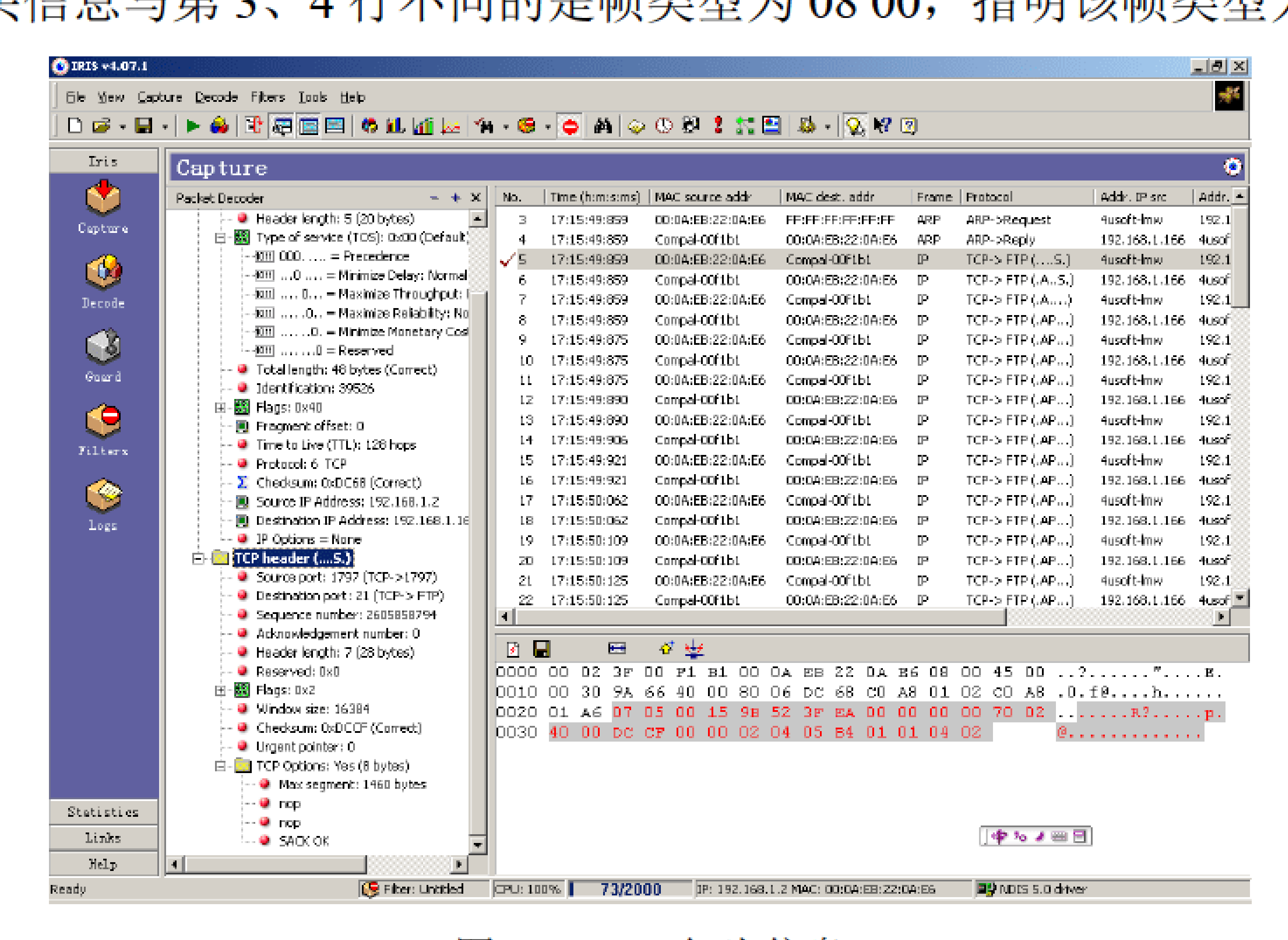


图 4-19　IP 包头信息

IP 协议是 TCP/IP 协议簇中最为核心的协议。所有的 TCP、UDP、ICMP 及 IGMP 数据都以 IP 数据报格式传输的，需要特别指出的是 IP 提供不可靠、无连接的数据报传送，也就是说 IP 仅提供最好的传输服务但不保证 IP 数据报能成功地到达目的地。保证数据正确到达目的地是 TCP 的工作。IP 协议头信息如图 4-20 所示。

<table>
<tr><th colspan="5">32位</th><th></th></tr>
<tr><td>4位版本</td><td>4位首部长度</td><td>8位服务类型 (TOS)</td><td colspan="2">16位总长度 (字节数)</td><td rowspan="5">20字节</td></tr>
<tr><td colspan="3">16位标识</td><td>3位标识</td><td>13位片偏移</td></tr>
<tr><td colspan="2">8位生存时间（TTL）</td><td>8位协议</td><td colspan="2">16位首部检验和</td></tr>
<tr><td colspan="5">32位源IP地址</td></tr>
<tr><td colspan="5">32位目的IP地址</td></tr>
<tr><td colspan="5">选项 (如果有)</td><td></td></tr>
<tr><td colspan="5">数据</td><td></td></tr>
</table>

图 4-20　IP 协议包头

IP 协议包头信息各个字段的说明如下。

> **提示：** 在包头信息中，各个字段的信息全部用十六进制数表示，一个数占 4 个二进制位，如 4 的二进制表示为 0100。

- 4 位版本

表示目前的协议版本号，数值是 4 表示版本为 4，因此 IP 有时也称作 IPv4。

- 4 位首部长度

头部的是长度，它的单位是 32 位(4 字节)，数值为 5 表示 IP 头部长度为 20 字节。

● 8 位服务类型(TOS)

这个 8 位字段由 3 位的优先权子字段，现在已经被忽略，4 位的 TOS 子字段以及 1 位的未用字段（现在为 0）构成。4 位的 TOS 子字段包含最小延时、最大吞吐量、最高可靠性以及最小费用，这四个 1 位最多只能有一个为 1，本例中都为 0，表示是一般服务。

● 16 位总长度

总长度字段是指整个 IP 数据报的长度，以字节为单位。数值为 00 30，换算成十进制为 48 字节，48 字节=20 字节的 IP 头+28 字节的 TCP 头，这个数据报只是传送的控制信息，还没有传送真正的数据，所以目前看到的总长度就是报头的长度。

● 16 位标识

标识字段唯一地标识主机发送的每一份数据报。通常每发送一份报文它的值就会加 1，第 5 行为数值为 9A 66，第 7 行为 9A 67，第 9 行为 9A 68。分片时涉及到标志字段和片偏移字段，本文不讨论这两个字段。

● 8 位生存时间（TTL）

TTL（time-to-live）生存时间字段设置了数据报可以经过的最多路由器数。它指定了数据报的生存时间。TTL 的初始值由源主机设置，一旦经过一个处理它的路由器，它的值就减去 1。可根据 TTL 值判断服务器是什么系统和经过的路由器。本例为 80，换算成十进制为 128，Windows 操作系统 TTL 初始值一般为 128，UNIX 操作系统初始值为 255，本例表示两个机器在同一网段且操作系统为 Windows。

● 8 位协议

表示协议类型，8 表示传输层是 TCP 协议。

● 16 位首部检验和

当收到一份 IP 数据报后，同样对首部中每个 16 位进行二进制反码的求和。由于接收方在计算过程中包含了发送方存在首部中的检验和，因此，如果首部在传输过程中没有发生任何差错，那么接收方计算的结果应该为全 1。如果结果不是全 1，即检验和错误，那么 IP 就丢弃收到的数据报。但是不生成差错报文，由上层去发现丢失的数据报并进行重传。

● 32 位源 IP 地址和 32 位目的 IP 地址

32 位的 IP 地址由一个网络 ID 和一个主机 ID 组成。本例源 IP 地址为 C0 A8 01 02，转换为十进制为 192.168.1.2; 目的 IP 地址为 C0 A8 01 A6，转换为十进制为 192.168.1.166。网络地址为 192.168.1，主机地址分别为 2 和 166，它们的网络地址是相同的，所以在一个网段内，这样数据在传送过程中可直接到达。

TCP 协议头信息如图 4-21 所示。

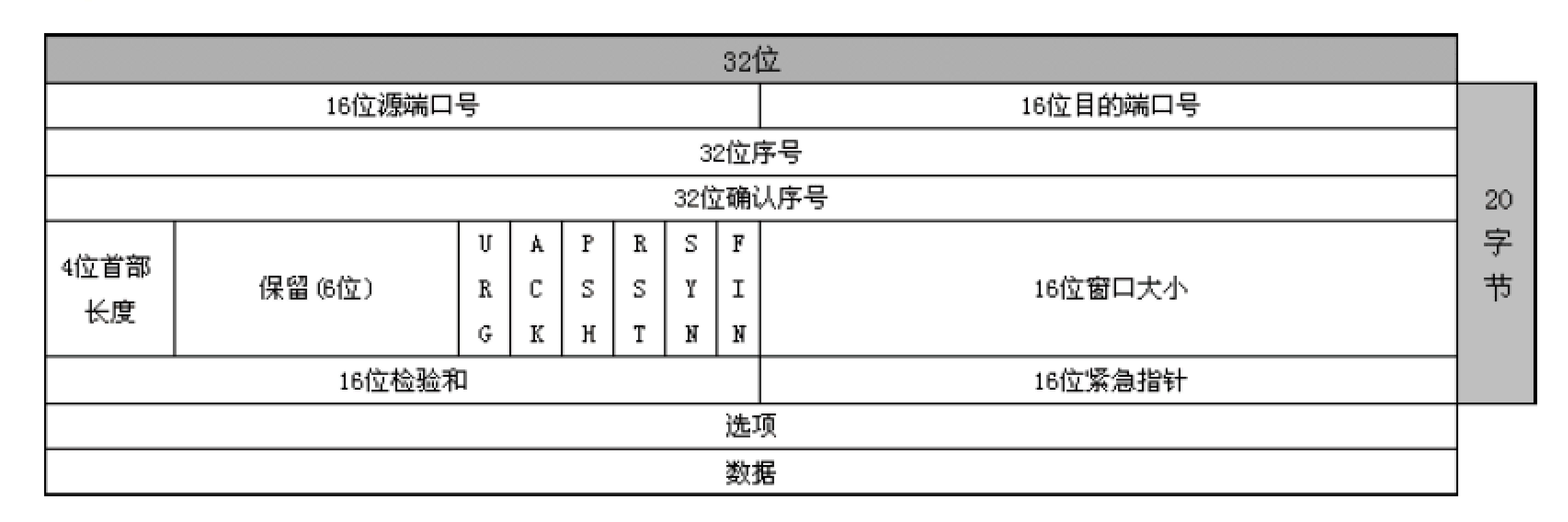


图 4-21　TCP 协议包头

第 5 行 TCP 的头信息是：07 05 00 15 9B 52 3F EA 00 00 00 00 70 02 40 00 DC CF 00 00 02 04 05 B4 01 01 04 02。

● 端口号

端口就像通道两端的门一样，当计算机之间进行通信时两端的门必须是打开的。源端口和目的端口各占 16 位，2 的 16 次方等于 65536，这就是每台电脑与其他电脑联系所能开的“门”。一般作为服务一方每项服务的端口号是固定的。本例目的端口号为 00 15，换算成十进制为 21，这正是 FTP 的默认端口，需要指出的是这是 FTP 的控制端口，数据传送时用另一端口，第三组的分析能看到这一点。客户端与服务器联系时随机开一个大于 1024 的端口，本例为 07 05，换算成十进制为 1797。

● 32 位序号

也称为顺序号（Sequence Number），简写为 SEQ，从上面三次握手的分析可以看出，当一方要与另一方联系时就发送一个初始序号给对方，意思是：“让我们建立联系吧？”服务方收到后要发个独立的序号给发送方，意思是“消息收到，数据流将以这个数开始。”由此可看出，TCP 连接完全是双向的，即双方的数据流可同时传输。在传输过程中双方数据是独立的，因此每个 TCP 连接必须有两个顺序号分别对应不同方向的数据流。

● 32 位确认序号

也称为应答号（Acknowledgment Number），简写为 ACK。在握手阶段，确认序号将发送方的序号加 1 作为回答，在数据传输阶段，确认序号将发送方的序号加发送的数据大小作为回答，表示确实收到这些数据。在第三组的分析中将看到这一过程。

● 4 位首部长度

这个字段占 4 位，每个数值代表 32 位（4 字节）。本例值为 7，TCP 的头长度为 28 字节，等于正常的长度 20 字节加上可选项 8 字节。TCP 的头长度最长可为 60 字节（二进制 1111 换算为十进制为 15，15*4 字节=60 字节）。

● 6 个标志位

URG 紧急指针，告诉接收 TCP 模块紧要指针域指着紧要数据。

ACK 置 1 时表示确认号，为 0 的时候表示数据段不包含确认信息，确认号被忽略。

PSH 置 1 时请求的数据段在接收方得到后就可直接送到应用程序，而不必等到缓冲区满时才传送。

RST 置 1 时重建连接。如果接收到 RST 位时候，通常发生了某些错误。

SYN 置 1 时用来发起一个连接。

FIN 置 1 时表示发送端完成发送任务。用来释放连接，表明发送方已经没有数据发送了。

● 16 位窗口大小

TCP 的流量控制由连接的每一端通过声明的窗口大小来提供。窗口大小为字节数，起始于确认序号字段指明的值，这个值是接收端正期望接收的字节。窗口大小是一个 16 字节字段，因而窗口大小最大为 65535 字节。

● 16 位检验和

检验和覆盖了整个的 TCP 报文段：TCP 首部和 TCP 数据。这是一个强制性的字段，一定是由发送端计算和存储，并由接收端进行验证。

● 16 位紧急指针

只有当 URG 标志置 1 时紧急指针才有效。紧急指针是一个正的偏移量，和序号字段中的值相加表示紧急数据最后一个字节的序号。

● 选项

最常见的可选字段是最长报文大小，又称为 MSS (Maximum Segment Size)。每个连接方通常都在握手的第一步中指明这个选项。它指明本端所能接收的最大长度的报文段。

3．数据传输

（1）显示数据包

84-87 行表示了一个数据传输的过程，如图 4-22 所示，这四行数据是数据传输过程中一个发送一个接收的过程。

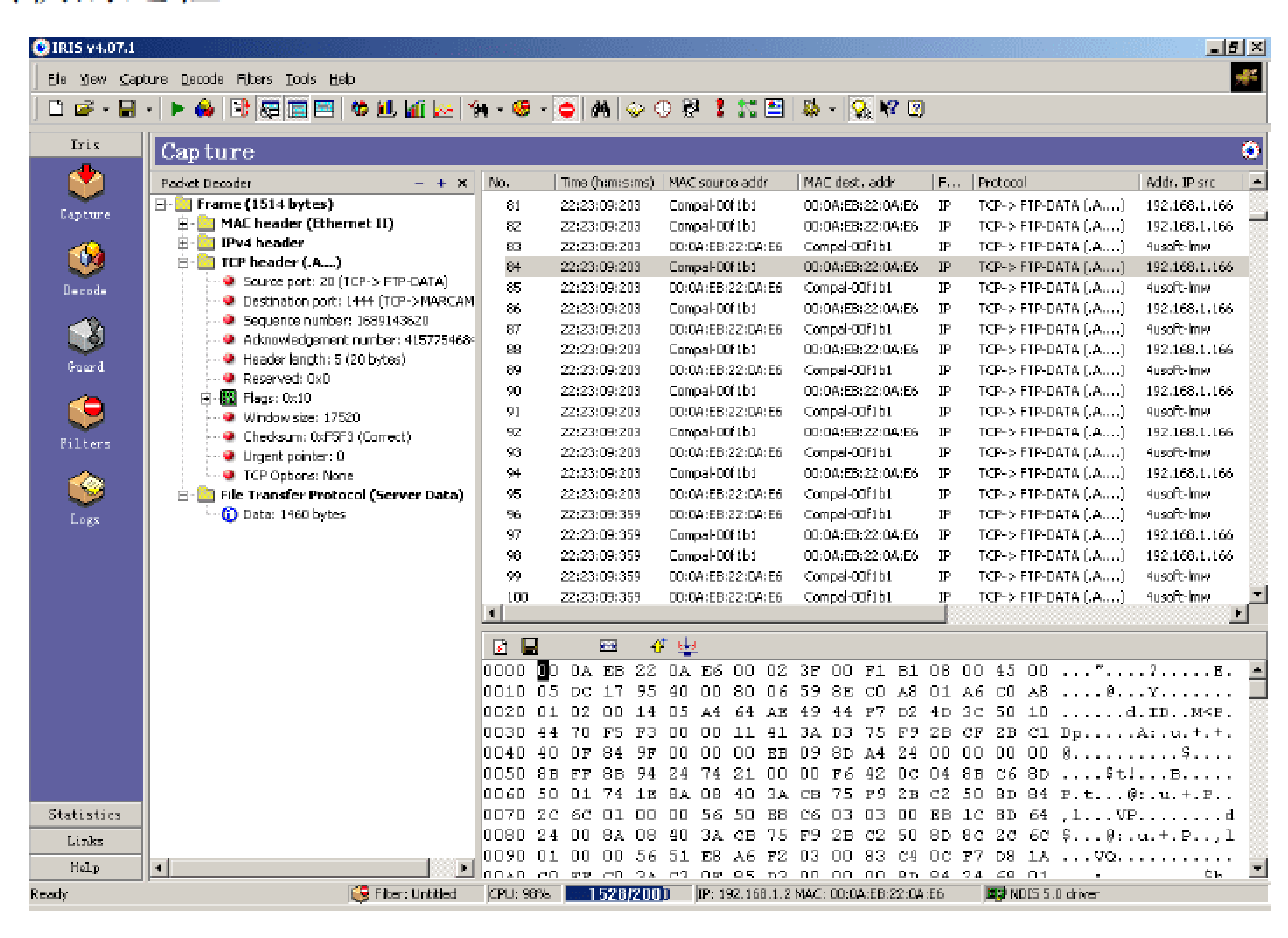


图 4-22　数据传输过程

（2）解释数据包

TCP 提供一种面向连接的、可靠的字节流服务。当接收端收到来自发送端的信息时，接收端要发送一条应答信息，表示收到此信息。数据传送时被 TCP 分割成认为最适合发送的数据块。一般以太网在传送时 TCP 将数据分为 1460 字节。也就是说数据在发送方被分成一块一块地发送，接收端收到这些数据后再将它们组合在一起。

84 行显示服务器给客户机发送了大小为 1514 字节大小的数据，注意我们前文讲过数据发送时是层层加协议头的，1514 字节=14 字节以太网头 + 20 字节 IP 头 + 20 字节 TCP 头 + 1460 字节数据。

85 行显示的应答信号 ACK 为 1689143620，这个数是 84 行的 SEQ 序号 1689142160 加上传送的数据 1460，客户机将这个应答信号发给服务器说明已收到发来的数据。

86、87 行显示的是继续传送数据的过程。

4．终止连接

（1）显示数据包

48-51 行的数据表示 TCP 连接的终止过程，如图 4-23 所示。

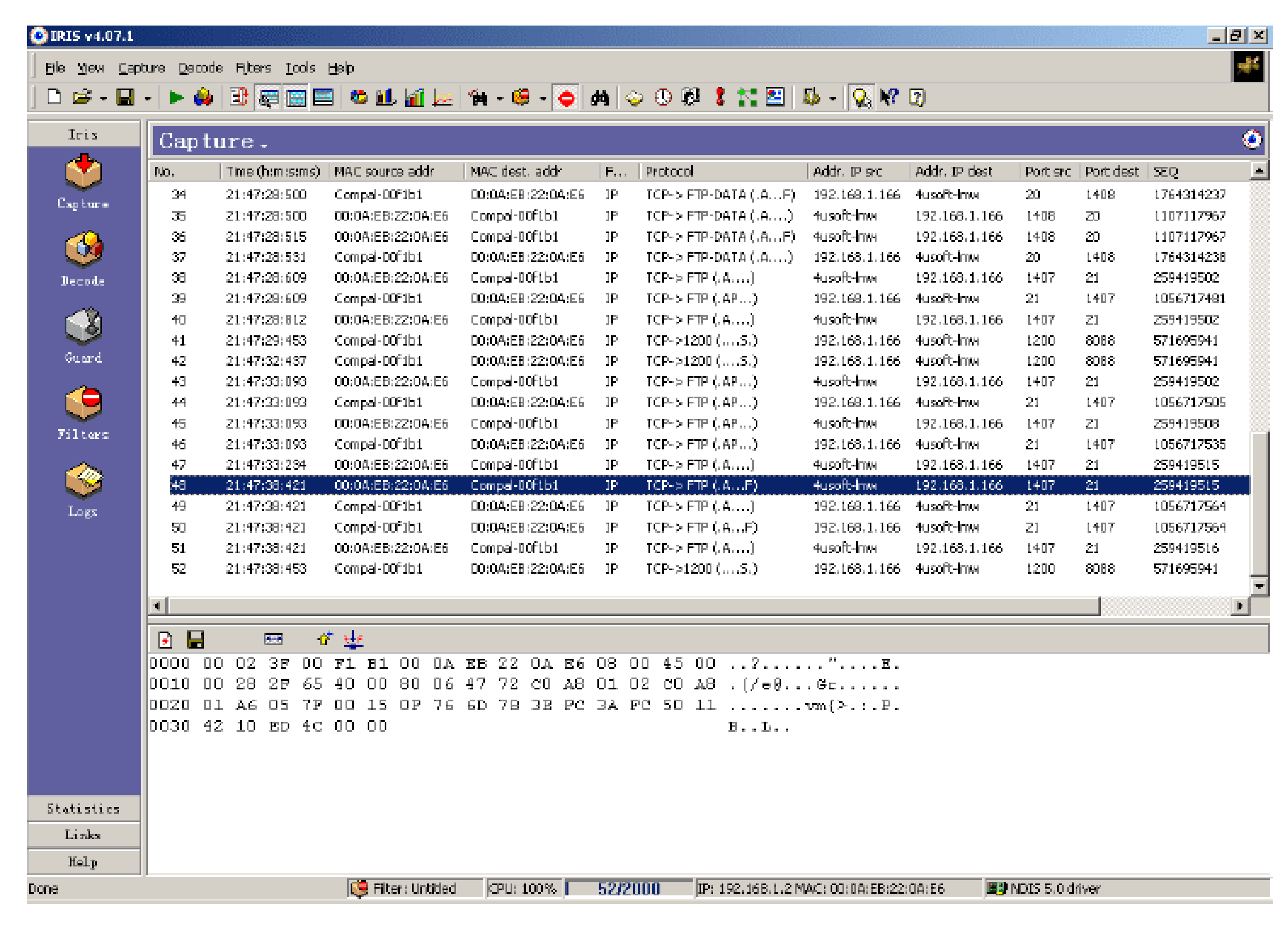


图 4-23 终止连接数据包

（2）解释数据包

建立一个连接需要三次握手，而终止一个连接要经过 4 次握手。这是因为一个 TCP 连接是全双工（即数据在两个方向上能同时传递），每个方向必须单独地进行关闭。4 次握手实际上就是双方单独关闭的过程。

文件下载完后，关闭浏览器终止了与服务器的连接，48-51 行显示的就是终止连接所经过 4 次握手过程。

48 行数据显示的是关闭浏览器后，客户机将 FIN 置 1 连同序号(SEQ)259419515 发给服务器请求终止连接。

49 行数据显示服务器收到 FIN 关闭请求后，发回一个确认，并将应答信号设置为收到序号加 1，这样就终止了这个方向的传输。

50 行数据显示服务器将 FIN 置 1 连同序号(SEQ)1056717564 发给客户机请求终止连接。

51 行数据显示客户机收到 FIN 关闭请求后，发回一个确认，并将应答信号设置为收到序号加 1，至此 TCP 连接彻底关闭。

4.3 包过滤防火墙

数据包过滤技术是在网络层对数据包进行选择，选择的依据是系统内设置的过滤逻辑，被称为访问控制表。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素，或它们的组合来确定是否允许该数据包通过。包过滤防火墙就是采用包过滤技术来实现的防火墙，下面对其相关知识进行介绍。

4.3.1 包过滤防火墙的一般概念

1. 包过滤防火墙定义

包过滤防火墙是用一个软件查看所流经的数据包的包头，由此决定整个数据包的命运。它可能会决定丢弃这个数据包，可能会接受这个数据包（让这个数据包通过），也可能执

行其他更复杂的动作。

在 Linux 系统下，包过滤功能是内建于核心的（作为一个核心模块，或者直接内建），同时还有一些可以运用于数据包之上的技巧，不过最常用的依然是查看包头以决定包的命运。

2. 包过滤防火墙的工作层次

包过滤是一种内置于 Linux 内核路由功能之上的防火墙类型，其防火墙工作在网络层。

4.3.2　包过滤防火墙的工作原理

（1）使用过滤器。数据包过滤用在内部主机和外部主机之间，过滤系统是一台路由器或是一台主机。过滤系统根据过滤规则来决定是否让数据包通过。用于过滤数据包的路由器被称为过滤路由器。

数据包过滤是通过对数据包的 IP 头和 TCP 头或 UDP 头的检查来实现的，主要信息有：

- IP 源地址
- IP 目标地址
- 协议（TCP 包、UDP 包和 ICMP 包）
- TCP 或 UDP 包的源端口
- TCP 或 UDP 包的目标端口
- ICMP 消息类型
- TCP 包头中的 ACK 位
- 数据包到达的端口
- 数据包出去的端口

在 TCP/IP 中，存在着一些标准的服务端口号，例如，HTTP 的端口号为 80。通过屏蔽特定的端口可以禁止特定的服务。包过滤系统可以阻塞内部主机和外部主机或另外一个网络之间的连接，例如，可以阻塞一些被视为是有敌意的或不可信的主机或网络连接到内部网络中。

（2）过滤器的实现。数据包过滤一般使用过滤路由器来实现，这种路由器与普通的路由器有所不同。

普通的路由器只检查数据包的目标地址，并选择一个达到目的地址的最佳路径。它处理数据包是以目标地址为基础的，存在着两种可能性：若路由器可以找到一个路径到达目标地址则发送出去；若路由器不知道如何发送数据包则通知数据包的发送者“数据包不可到达”。

过滤路由器会更加仔细地检查数据包，除了决定是否有到达目标地址的路径外，还要决定是否应该发送数据包。“应该与否”是由路由器的过滤策略决定并强制执行的。

路由器的过滤策略主要有：

- 拒绝来自某主机或某网段的所有连接。
- 允许来自某主机或某网段的所有连接。
- 拒绝来自某主机或某网段的指定端口的连接。
- 允许来自某主机或某网段的指定端口的连接。
- 拒绝本地主机或本地网络与其他主机或其他网络的所有连接。

- 允许本地主机或本地网络与其他主机或其他网络的所有连接。
- 拒绝本地主机或本地网络与其他主机或其他网络的指定端口的连接。
- 允许本地主机或本地网络与其他主机或其他网络的指定端口的连接。

4.3.3 包过滤器操作的基本过程

下面对包过滤器操作过程做个简单的叙述。

（1）包过滤规则必须被包过滤设备端口存储起来。

（2）当包到达端口时，对包报头进行语法分析。大多数包过滤设备只检查 IP、TCP、或 UDP 报头中的字段。

（3）包过滤规则以特殊的方式存储。应用于包的规则的顺序与包过滤器规则存储顺序必须相同。

（4）若一条规则阻止包传输或接收，则此包便不被允许。

（5）若一条规则允许包传输或接收，则此包便可以被继续处理。

（6）若包不满足任何一条规则，则此包便被阻塞。

4.3.4 包过滤技术的优缺点

1. 包过滤技术的优点

（1）对于一个小型的、不太复杂的站点，包过滤比较容易实现。

（2）因为过滤路由器工作在 IP 层和 TCP 层，所以处理包的速度比代理服务器快。

（3）过滤路由器为用户提供了一种透明的服务，用户不需要改变客户端的任何应用程序，也不需要用户学习任何新的东西。因为过滤路由器工作在 IP 层和 TCP 层，而 IP 层和 TCP 层与应用层的问题毫不相关。所以，过滤路由器有时也被称为“包过滤网关”或“透明网关”，之所以被称为网关，是因为包过滤路由器和传统路由器不同，它涉及到了传输层。

（4）过滤路由器在价格上一般比代理服务器便宜。

2. 包过滤技术的缺点

（1）一些包过滤网关不支持有效的用户认证。

（2）规则表很快会变得很大而且复杂，规则很难测试。随着表的增大和复杂性的增加，规则结构出现漏洞的可能性也会增加。

（3）这种防火墙最大的缺陷是它依赖一个单一的部件来保护系统。如果这个部件出现了问题，会使得网络大门敞开，而用户其至可能还不知道。

（4）在一般情况下，如果外部用户被允许访问内部主机，则它就可以访问内部网上的任何主机。

（5）包过滤防火墙只能阻止一种类型的 IP 欺骗，即外部主机伪装内部主机的 IP，对于外部主机伪装外部主机的 IP 欺骗却不可能阻止，而且它不能防止 DNS 欺骗。

虽然，包过滤防火墙有如上所述的缺点，但是在管理良好的小规模网络上，它能够正常地发挥其作用。一般情况下，人们不单独使用包过滤网关，而是将它和其他设备（如堡垒主机等）联合使用。

4.4　代理防火墙

代理防火墙，也称应用层防火墙，作用于应用层。其核心是运行于防火墙主机上的代理服务器进程，它代替网络用户完成特点的 TCP/IP 功能。一个代理服务器实际上是一个为特定网络应用而连接两个网络的网关，对于每一种不同的应用服务，都必须有一个相应的代理。外部网络和内部网络之间要建立连接，必须通过代理的中间转换，内部网络只接受代理服务提出的服务请求，拒绝外部网络的直接连接，从而达到保护内部网络的目的。

4.4.1　为什么要进行代理

如果用户不能访问 Internet，那么与其连接就没有意义。另一方面，若你的系统中的所有主机都能自由地访问 Internet，则在与 Inernet 网连接时将没有安全感。对于这种情况，现在已经提出一些方案来解决这个问题。

最为有效的办法是为所有的用户提供一台主机与因特网连接（但这并不是令人满意的方案），因为这些主机对用户来说是不透明的，那些想访问因特网的用户将无法直接访问，他们不得不在双重宿主主机上登录，并从那里访问因特网，然后将结果送回到他们自己的主机，这种多步处理方法要使用户进行多次传送并且离开他们所熟悉的环境。

对于一个具有多操作系统的站点来说情况将更糟糕，如果你的本地系统是 Macintosh，而你的双重宿主主机是 UNIX 系统，而 UNIX 系统可能太陌生了。这样你将受到各种限制，因为 UNIX 系统中的工具与你在自己的主机上使用的工具可能完全不同。

没有配置代理系统的双重宿主主机对于利用它来访问因特网的用户来说，会大大降低他们所获得的效益。另外，它一般难以提供足够的安全机制来保护系统，特别是对于要与外界连接的主机。

代理系统不会受到双重宿主主机不安全机制的影响，它们通过与双重宿主主机的相互作用来解决安全问题。代理系统要求用户在后台与双重宿主主机进行交谈而不能直接在双重宿主主机上进行。由于用户很少与双重宿主主机进行交谈，所以用户根本感觉不到代理的存在，他们认为自己是在直接访问因特网服务器。如图 4-24 所示。

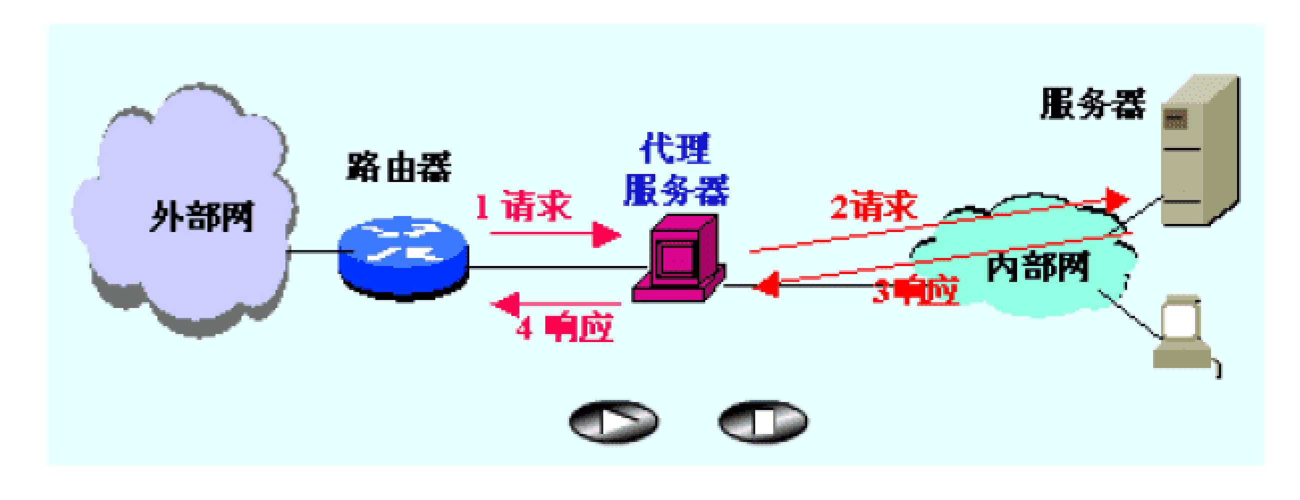


图 4-24　代理系统的实现过程

代理系统通过避免用户在双重宿主主机上登录和强迫通过控制软件连接来解决安全问题。因为代理软件的运行不需要用户登录到双重宿主主机，它所运行的主机由于没有随意地登录而得到了安全。人们无法不安装控制软件而访问因特网，代理就是这样一个控制系统。

4.4.2 代理服务的优缺点

1．代理服务有两个优点

（1） 代理服务允许用户“直接”访问因特网

采用双重宿主主机的方案，用户需要登录到主机上才能访问因特网，这样会使用户感到很不方便，有些用户就可能寻找其他方法来通过防火墙。而采用代理服务，用户会认为他们是直接访问因特网。

当然这需要在后台运行一些程序，但这对用户来讲是透明的。代理服务系统允许用户从他们自己的系统访问因特网，但不允许数据包在用户系统和因特网之间直接传送。传送只能是间接的，或通过双重宿主主机，或通过一个堡垒主机和屏蔽路由器系统。

（2） 代理服务适合于做日志

因为代理服务懂得优先协议，它们允许日志服务以一种特殊且有效的方式来进行。比如一个 FTP 代理服务器只记录发出的命令和服务器接收的回答，用这种方法来代替记录所有的数据传输，这样产生的日志就会小而有用。

2．代理服务的缺点

代理服务也有一些缺点，主要表现如下。

（1）代理服务落后于非代理服务

尽管代理软件已广泛应用于一些老而旧的服务，如 Telnet 和 FTP 等，但是要找到一些为了某些新而少的服务使用的可靠软件是很困难的。在一个服务出现和它的代理服务的出现之间一般会有一个较为明显的延迟，这个延迟时间的长短是依赖于为代理而设计的服务器的。这使得一个站点在提供一个新的服务时无法立刻提供代理服务，在可以使用代理服务之前，该服务只能不放在防火墙内，这样一来就有安全漏洞产生。

（2）每个代理服务要求不同的服务器

用户可能需要为每个协议配置不同的代理服务器，因为代理服务器需要按照协议来决定允许什么和不允许什么，并且要扮演一个角色，它对真实服务器来说是客户，对客户来说是真实服务器。因此选择、安装和配置这些不同的代理服务器是一项复杂的工作。

软件产品和软件包在配置的难易程度上是完全不同的，在一个软件上很容易做的可能在另一个软件上就非常难。例如，那些特别容易配置的服务器通常灵活性要差一些，它们能容易地配置是因为对如何使用它们作了各种假定，这些假定对于你的站点来说可能是合适的也可能是不合适的。

（3）代理服务一般要求对客户或程序进行修改

除了一些专门为代理而设计的服务外，代理服务器要求对客户或程序进行修改，每一种修改都有其不足之处，人们无法总是用正常的方式来进行工作。因为这些修改，代理应用就可能没有非代理应用运行得那样好，同时对于协议的理解也可能有偏差，并且一些客户程序和服务器要比非代理服务缺乏灵活性。

（4）代理服务对某些服务来说是不合适的

代理服务能否实现取决于能否在客户和真实服务器之间插入代理服务器，这要求两者间的交谈有相对的直接性。一个像 talk 这样复杂的交谈可能永远无法进行代理。

（5）代理服务不能保护你不受协议本身缺点的限制

作为一个确保安全的方案，代理首先要判断对协议中哪些操作是安全的，但并不是所有的协议都能方便地做到这一点，如 X Window 系统协议中就存在许多不安全的操作，假如禁止这些不安全的操作系统就不能正常地运行了。

4.4.3　代理服务的工作方法

代理服务的工作细节对每一种服务都是不同的，一些服务可以容易或者自动地提供代理，对于这些服务你可以通过对正常服务器的配置来设置代理。但对于大多数服务来说，代理服务在服务器上要求有合适的代理服务器软件。在客户端可以有不同的方法。

（1）定制客户软件。采用这种方法，软件必须知道当用户提出请求时怎样与代替真实服务器的代理服务器进行连接，并且告诉代理服务器如何与真实服务器连接。

（2）定制客户过程。采用这种方法时，用户使用标准的客户软件与代理服务器连接，并通知代理服务器与真实服务器连接，以此来代替与真实服务器的连接。

1. 使用定制客户软件进行代理

第一个方法是使用定制客户软件进行代理，这种方法存在一些问题。定制的客户软件一般只适用于特定的平台。如果它对你的站点中一个平台都不适合的话，那么你的用户就太不幸了。

有时虽然定制客户软件适合你的平台，但它并不是用户所想要的，如在 Macintosh 上有许多 FTP 客户程序，其中有的具有很好的用户界面，另外也有些很有用的功能，如 anarchie 是一个可以将 Archie 客户与 FTP 客户合并成一个程序的界面，这样你就可以在一个用户界面中利用 Archie 查找文件，再用 FTP 进行文件下载。如果你想使用的软件不支持你的代理服务器，那也不行。有时你可以修改客户程序来支持代理服务器，但这需要有客户程序的源程序，并有重新编译能力，一般很少有客户程序支持任何形式的代理系统。

对于这种情况的例外是 WWW 的客户程序如 Mosaic。很多这样的程序支持各种类型的代理（特别是 SOCKS 和 CREN HTTP 守护程序），大多数都是在防火墙和代理系统普及之后新出现的，因此知道了运行环境，并且在设计开始时就考虑了代理问题。

把客户程序进行修改后用于代理系统则不能使代理做到对用户透明。许多站点在内部使用原先未修改的客户程序，而在外部连接上使用修改的客户程序，用户必须要记住使用修改的客户程序来进行外部连接。这就往往使得用户按照他们已熟悉的步骤进行连接时，可能会在内部成功而连接外部时则失败。

此外还要选择正确的程序，用户可能会发现自己要进行额外的配置，因为客户程序需要了解怎样与代理服务器相连。这虽然不是一个复杂的工作，但却增加了出错的机会。

2. 使用定制的用户过程进行代理

使用定制用户过程的方法，代理服务器使用标准的软件来工作,然而,它们要求软件的用户遵守定制的过程。用户通知客户与代理服务器连接并通知代理服务器与哪个主机相连接。因为几乎没有一个协议是设计成传递这种信息的，用户不仅需要记住代理服务器的名字，而且还要记住通过其他主机名字的特殊方式。

它是如何工作的？你需要告诉自己的用户每个协议的具体步骤。如 FTP 协议，假定用户想从匿名 FTP 服务器（ftp.getfile.net）上下载一个文件，则应该：

（1）使用一 FTP 客户与代理服务器进行连接而不是与匿名 FTP 服务器直接连接。

（2）在输入用户名时，除了指定用户名的同时，还要指定他想要连接的真实的服务器名。例如，要连接匿名 FTP 服务器（ftp.getfile.net），那么在代理服务器上需输入 anonymous@ftp.getfile.net，而不应只输入“anonymous”。

正如使用定制软件一样，要求对用户使用过程进行定制，使用定制过程也会对你可使用的客户程序增加一些限制。有的客户试图自动执行匿名 FTP，但他们不知道如何经过代理服务器。一些客户可能被简单的操作方式所困扰，如一个图形界面的程序可能无法显示用户输入的包括主机和用户名的信息。

4.4.4 代理服务器的使用

代理服务器有一些特殊类型，主要表现如下。

1. 应用级与回路级代理

应用级代理是已知代理服务为哪个应用提供的代理，它能了解并解释应用协议中的命令，而回路级代理在客户端与服务器之间不解释应用协议中的命令就建立了连接回路。大多数应用级代理的最新版本是一个像 sendmail 的应用，由它来完成存储转发协议。大部分最新回路级代理是一个新式的代理网关，这个网关对外像一个代理，对内像一个过滤路由器。

应用级代理使用修改的过程，回路级代理使用修改的客户程序。这与代理的实用性有关。为了实现一个代理连接，你必须知道连接的方向。一个混合网关可以很容易地阻止连接，但一个代理主机只能接收连接，并从得到的信息中判断它要往哪里继续进行连接。一个回路级代理不能解释应用协议，需要通过其他方式给它提供信息。因为客户程序的能力是很有效的，应用级代理通常是为了利用它们了解应用协议的优点，因此它们能使用修改的过程。而回路级代理，通常无法使用修改的过程，只能使用修改的客户程序。

尽管还没有修改的应用级代理，但确实存在着修改的回路级代理，如 plug gw 就是一个修改的过程并且是一个回路级代理。它连接的目标地址完全取决于源地址和与之连接的源及目标端口。

一个回路级代理的优点在于它能够为各种不同的协议提供服务。大多数回路级代理服务器也是公共代理服务器，它们几乎对于任何协议都支持，但不是每个协议都能由回路级代理轻易实现的，如 FTP 协议就是这样。它要求从客户端的数据端口连接到服务器上，并要求作协议级的调整和应用级的知识。回路级代理的缺点在于它对因代理而产生的事件几乎无法控制，像包过滤一样，它为源地址和目的地址提供连接，但是不能判断出经过它的命令是否安全或超出了协议的范围。回路级代理会很容易地被服务器设置的、分给其他服务器的端口号所蒙骗。

2. 公共与专用代理服务器

虽然“应用级”和“回路级”是常用的术语，但是我们更加注重“公共”和“专用”代理服务器的区别。一个专用代理服务器只适用于单个协议，而一个公共代理服务器则适用多个协议。实际上专用代理服务器是应用级的，而公共代理服务器是属于回路级的。由于存在一个了解许多协议的公共的应用级代理服务器，或一个专用的回路级代理服务器（只提供一个服务，但了解多个协议），因此采用“专用”和“公共”这两个术语要比“应用

级”和“回路级”好理解一些。

3．智能代理服务器

如果一个代理服务器不光是转发请求，同时还能够做其他许多事情的话，这样的代理服务器就称为智能代理服务器，如 CERN HTTP 代理服务器还能够将数据保存在缓存中，以便同样的数据可以不必再从因特网上下载了。代理服务器（特别是应用级代理服务器）可以比其他方式提供更好的日志和访问控制功能。代理服务器的功能在不断迅速地发展，现在已有许多代理服务器除了提供基本功能外，还在不断增加新的功能。对于一个专用的应用级代理来说很容易升级到智能代理服务器，但对一个回路级的代理来说则较为困难。

4.5　防火墙技术的发展趋势

随着新的网络攻击的出现，防火墙技术也有一些新的发展趋势。这主要可以从包过滤技术、防火墙体系结构和防火墙系统管理三方面来体现。

4.5.1　防火墙包过滤技术发展趋势

（1）引入身份认证

一些防火墙厂商把在 AAA 系统上运用的用户认证及其服务扩展到防火墙中，使其拥有可以支持基于用户角色的安全策略功能。该功能在无线网络应用中非常必要。具有用户身份验证的防火墙通常是采用应用级网关技术的，包过滤技术的防火墙不具有。用户身份验证功能越强，它的安全级别越高，但它给网络通信带来的负面影响也越大，因为用户身份验证需要时间，特别是加密型的用户身份验证。

（2）多级过滤技术

所谓多级过滤技术，是指防火墙采用多级过滤措施，并辅以鉴别手段。在分组过滤（网络层）一级，过滤掉所有的源路由分组和假冒的 IP 源地址；在传输层一级，遵循过滤规则，过滤掉所有禁止出或/和入的协议和有害数据包如 nuke 包、圣诞树包等；在应用网关（应用层）一级，能利用 FTP、SMTP 等各种网关，控制和监测 Internet 提供的所用通用服务。这是针对以上各种已有防火墙技术的不足而产生的一种综合型过滤技术，它可以弥补以上各种单独过滤技术的不足。

这种过滤技术在分层上非常清楚，每种过滤技术对应于不同的网络层，从这个概念出发，又有很多内容可以扩展，为将来的防火墙技术发展打下基础。

（3）使防火墙具有病毒防护功能。现在通常被称之为“病毒防火墙”，当然目前主要还是在个人防火墙中体现，因为它是纯软件形式，更容易实现。这种防火墙技术可以有效地防止病毒在网络中的传播，比等待攻击的发生更加积极。拥有病毒防护功能的防火墙可以大大减少公司的损失。

4.5.2　防火墙的体系结构发展趋势

随着网络应用的增加，对网络带宽提出了更高的要求。这意味着防火墙要能够以非常高的速率处理数据。另外，在以后几年里，多媒体应用将会越来越普遍，它要求数据穿过防火墙所带来的延迟要足够小。为了满足这种需要，一些防火墙制造商开发了基于 ASIC

的防火墙和基于网络处理器的防火墙。从执行速度的角度看来，基于网络处理器的防火墙也是基于软件的解决方案，它需要在很大程度上依赖于软件的性能，但是由于这类防火墙中有一些专门用于处理数据层面任务的引擎，从而减轻了 CPU 的负担，该类防火墙的性能要比传统防火墙的性能好许多。

与基于 ASIC 的纯硬件防火墙相比，基于网络处理器的防火墙具有软件色彩，因而更加具有灵活性。基于 ASIC 的防火墙使用专门的硬件处理网络数据流，比起前两种类型的防火墙具有更好的性能。但是纯硬件的 ASIC 防火墙缺乏可编程性，这就使得它缺乏灵活性，从而跟不上防火墙功能的快速发展。理想的解决方案是增加 ASIC 芯片的可编程性，使其与软件更好地配合。这样的防火墙就可以同时满足来自灵活性能和运行性能的要求。

首信 CF-2000 系列 EP-600 和 CG-600 高端千兆防火墙即采用了功能强大的可编程专有 ASIC 芯片作为专门的安全引擎，很好地兼顾了灵活性能的需要。它们可以以线速处理网络流量，而且其性能不受连接数目、包大小以及采用何种策略的影响。该款防火墙支持 QoS，所造成的延迟可以达到微秒量级，可以满足各种交互式多媒体应用的要求。浙大网新也在杭州正式发布三款基于 ASIC 芯片的网新易尚千兆系列网关防火墙，据称，其 ES4000 防火墙速度达到 4Gbps，3DES 速度可达 600Mbps。易尚系列千兆防火墙还采用了最新的安全网关概念,集成了防火墙、VPN、IDS、防病毒、内容过滤和流量控制等多项功能。

4.5.3 防火墙的系统管理发展趋势

防火墙的系统管理也有一些发展趋势，主要体现在以下几个方面。

（1）首先是集中式管理，分布式和分层的安全结构是将来的趋势。集中式管理可以降低管理成本，并保证在大型网络中安全策略的一致性。快速响应和快速防御也要求采用集中式管理系统。目前这种分布式防火墙早已在 Cisco（思科）、3Com 等大的网络设备开发商中开发成功，也就是目前所称的“分布式防火墙”和“嵌入式防火墙”。关于这一新技术在本篇下面将详细介绍。

（2）强大的审计功能和自动日志分析功能。这两点的应用可以更早地发现潜在的威胁并预防攻击的发生。日志功能还可以使管理员有效地发现系统中存的安全漏洞，及时地调整安全策略等各方面管理具有非常大的帮助。不过具有这种功能的防火墙通常是比较高级的，早期的静态包过滤防火墙是不具有的。

（3）网络安全产品的系统化

随着网络安全技术的发展，现在有一种提法，叫做“建立以防火墙为核心的网络安全体系”。因为我们在现实中发现，仅现有的防火墙技术难以满足当前网络安全需求。通过建立一个以防火墙为核心的安全体系，就可为内部网络系统部署多道安全防线，各种安全技术各司其职，从各方面防御外来入侵。

如现在的 IDS 设备就能很好地与防火墙一起联合。一般情况下，为了确保系统的通信性能不受安全设备的影响太大，IDS 设备不能像防火墙一样置于网络入口处，只能置于旁路位置。而在实际使用中，IDS 的任务往往不仅在于检测，很多时候在 IDS 发现入侵行为以后，也需要 IDS 本身对入侵及时遏止。显然，要让处于旁路侦听的 IDS 完成这个任务又太难了，同时主链路又不能串接太多类似设备。在这种情况下，如果防火墙能和 IDS、病毒检测等相关安全产品联合起来，充分发挥各自的长处，协同配合，共同建立一个有效的

安全防范体系，那么系统网络的安全性就能得到明显提升。

目前主要有两种解决办法：一种是直接把 IDS、病毒检测部分直接“做”到防火墙中，使防火墙具有 IDS 和病毒检测设备的功能；另一种是各个产品分立，通过某种通信方式形成一个整体，一旦发现安全事件，则立即通知防火墙，由防火墙完成过滤和报告。目前更看重后一种方案，因为它的实现方式较前一种容易许多。

4.6　防火墙应用

1. 防火墙选择原则

防火墙是网络安全基础设施之一，根据不同的网络规模、网络结构以及网络应用，对于防火墙功能和性能的需求也不尽相同，那么，应该如何选择合适的防火墙呢？下面给出一个简单的指导。

（1）防火墙的管理难易度是防火墙能否达到目的的主要考虑因素之一。若防火墙的管理过于困难，则可能会造成设定上的错误，反而不能达到其功能。一般企业之所以很少用已有的网络设备直接当作防火墙的原因，除了先前提到的包过滤并不能达到完全的控制之外，设置工作困难，要具备完整的知识以及不易除错等管理问题更是一般企业不愿意使用的主要原因。

（2）防火墙也是网络上的主机之一，也可能存在安全问题。防火墙如果不能确保自身安全，则防火墙的控制功能再强，也终究不能完全保护内部网络。如果防火墙控制机制失效，则一个黑客可能取得防火墙上的控制权，然后几乎可以为所欲为地修改防火墙上的存取规则，进而侵入更多的系统。

（3）防火墙具有不同级别的安全等级规范。最著名的就是美国国家安全局的国家计算机安全中心颁的官方标准——桔皮书，其正式名称是“受信任电脑系统评价标准”，它将一个计算机系统可接受的信任程度予以分级，依安全性由高到低划分为 A B C D 四个等级，其中这些安全等级不是线性的，而是以指数级上升的。选择防火墙时要注意其安全等级规范指标。

（4）好的防火墙必须能弥补操作系统的不足。一个好的防火墙必须是建立在操作系统的底层而不是操作系统的上层，所以操作系统的漏洞可能并不会影响到一个好的防火墙系统所提供的安全性。相反，一个好的防火墙系统可以弥补操作系统的不足。

（5）一个好的防火墙不但本身要有良好的运行效率，还应该提供多平台的运行方式供使用者选择。由于防火墙并非完全由硬件构成，所以软件所提供的功能以及运行效率一定会影响到整体的表现，而使用者的操作意愿及熟悉程度也是必须考虑的重点。毕竟使用者才是完全的控制者，应该选择一套符合现有环境需求的软件，而并非为了软件的限制而改变现在的环境。

（6）一个好的防火墙就必须有一个完善的售后服务作为使用者的安全后盾。由于有新的产品出现，就会有人研究新的破解方法，所以一个好的防火墙提供者就必须有一个强大的服务组织作为使用者的安全后盾，也应该有众多的使用者所建立的口碑为防火墙作见证。

（7）企业安全政策中的一些特殊需求也要作为选择防火墙的一个标准。企业安全政策

中往往有些特殊需求不是每一个防火墙都会提供的，这方面常会因此成为选择防火墙的考虑因素之一。

2．个人防火墙举例

为了进一步了解个人防火墙的功能以及使用方法，在此以天网防火墙为例，说明个人防火墙的功能以及使用方法。

应用程序网络访问规则设置的具体操作如下。

（1）选择“开始”|“程序”|“天网防火墙”|“天网防火墙”命令，出现“天网防火墙个人版”窗口，如图 4-25 所示。

（2）当有程序需要和网络上的其他程序进行通信时，天网防火墙会出现提示窗口，提示配置对该程序的通信策略，如图 4-26 所示。



图 4-25　天网防火墙界面

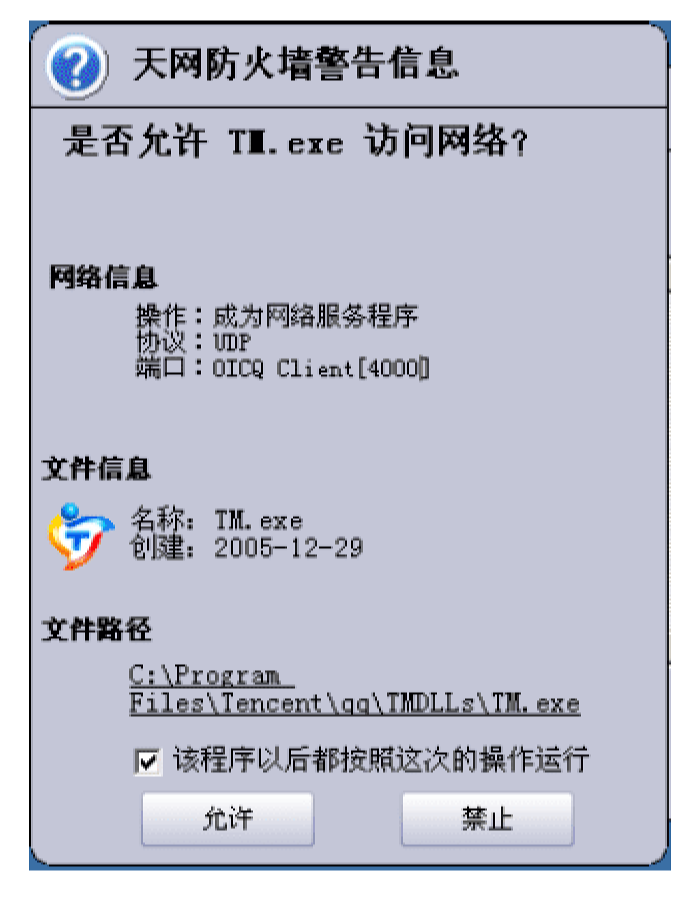


图 4-26　警告信息窗口

（3）如果需要通信的程序是合法程序，这时可以选择“该程序以后都按照这次的操作运行”复选框，然后单击“允许”按钮，如果需要通信的程序是非法程序，同样选择“该程序以后都按照这次的操作运行”复选框，然后单击“禁止”按钮，不管是单击“允许”还是“禁止”按钮，都会增加一条应用程序通信规则。在“天网防火墙”窗口上单击“应用程序规则”，如图 4-27 所示。

（4）每项应用程序规则都针对一个应用程序的通信控制策略，可以设置运行通信、禁止通信以及通信时提示三种方式，设置方法是通过单击应用程序规则项目右侧的对勾、问号或者叉，对勾表示允许通信，问号表示每次通信时询问，然后根据应答结果来决定是否通信，叉表示禁止通信。除此以外，还可以单击“选项”按钮，出现更详细的高级设置选项，如图 4-28 所示。

（5）根据需要完成设置以后，单击“确定”按钮，使设置生效。

除了上述的按照应用程序设置规则以外，天网防火墙还提供了一种按照 IP 规则来配置通信策略，而不管是什么应用程序进行通信，这样从某种程度上简化了配置过程。

IP 规则设置的具体操作如下。

（1）选择“开始”|“程序”|“天网防火墙”|“天网防火墙”命令，出现“天网防火

墙个人版”窗口，如图 4-25 所示。

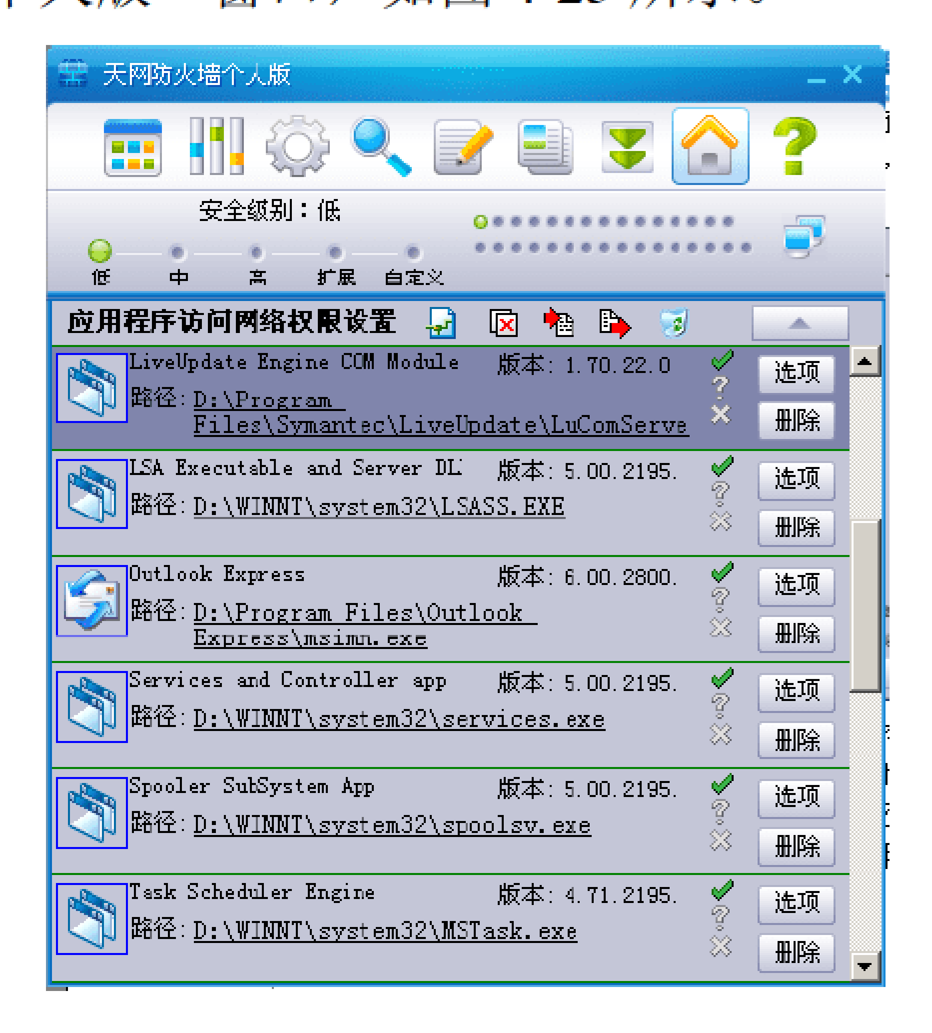


图 4-27　应用程序规则

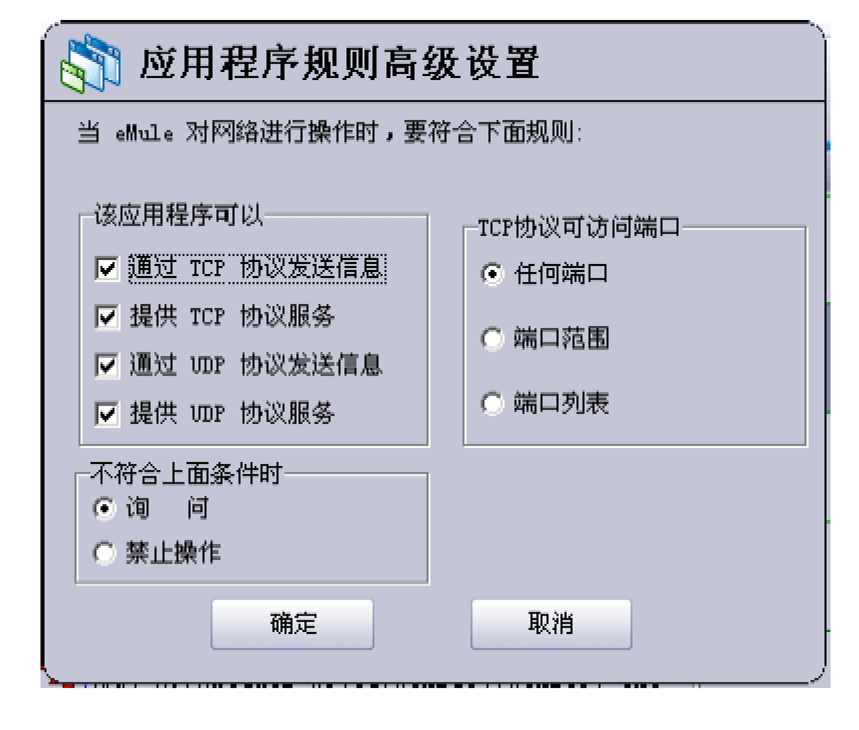


图 4-28　应用程序规则高级设置

（2）在“天网防火墙”窗口上单击“IP 规则管理”，出现如图 4-29 所示窗口。

（3）单击规则列表中复选框，可以设置对应规则是否有效，有效的规则显示为黑色字体，而且前面的复选框为选中状态，无效规则显示为浅灰色字体，复选框没有被选中。双击规则列表中的“允许自己用 ping 命令探测其他机器”规则，出现规则的详细信息，如图 4-30 所示，然后可以对这些规则进行修改。

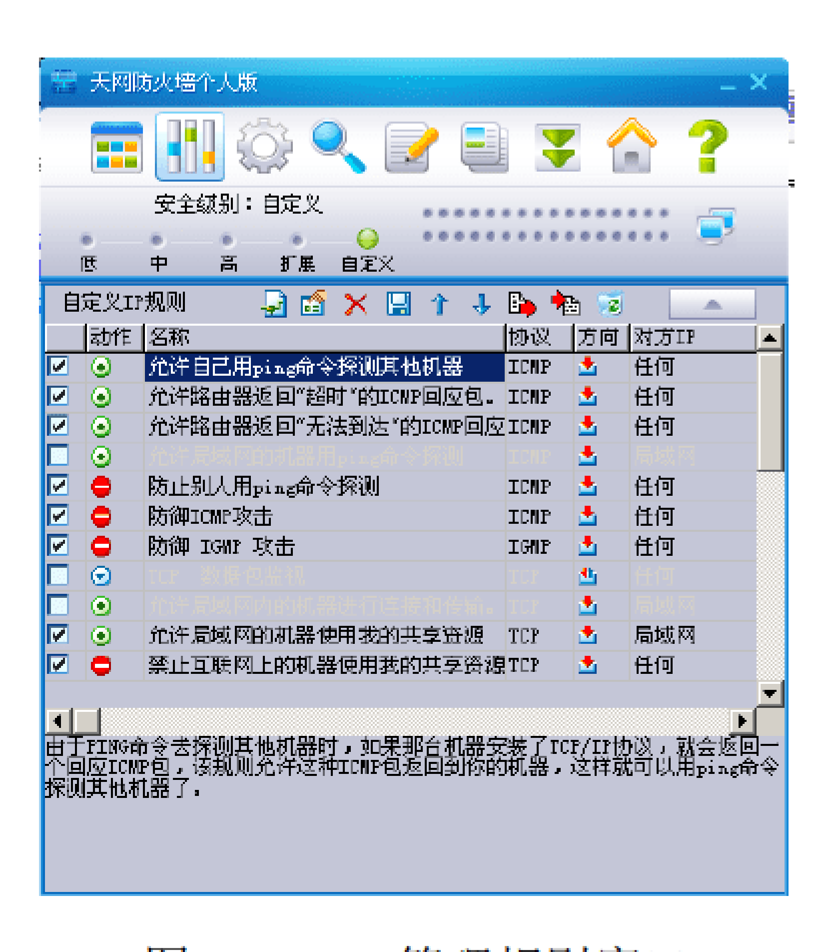


图 4-29　IP 管理规则窗口

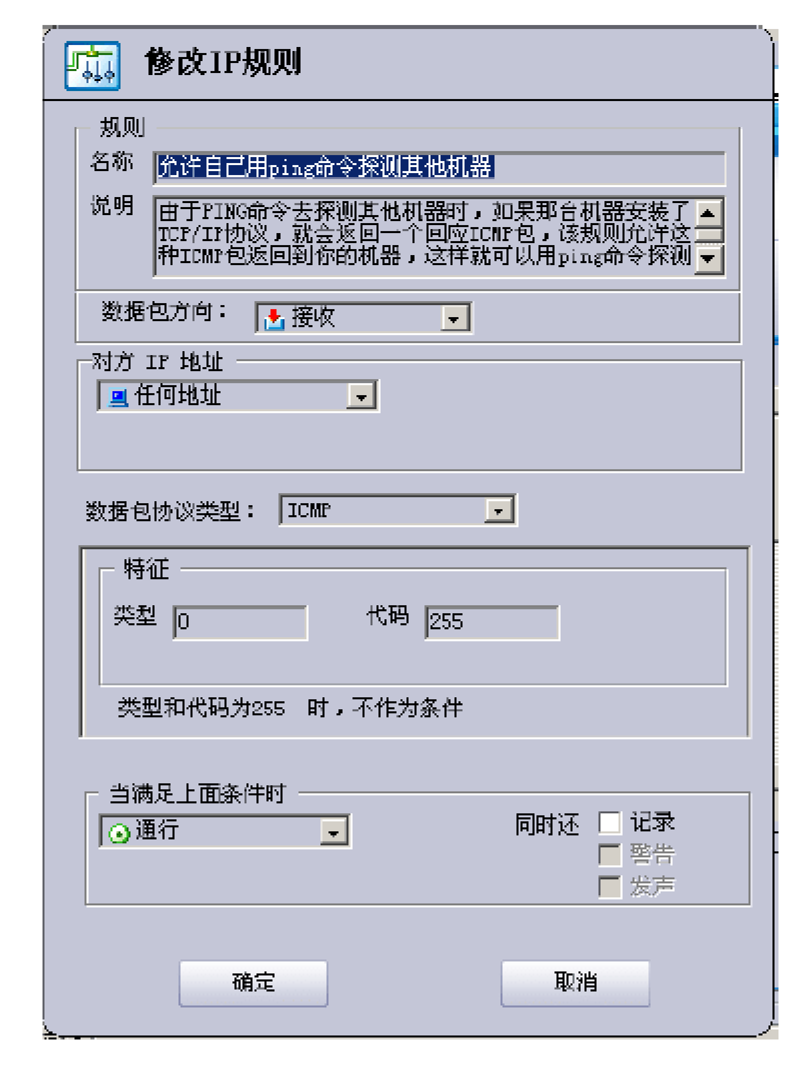


图 4-30　修改 IP 规则对话框

（4）在“当满足上面条件时”的下拉列表框中选择“通行”，进行 Ping 探测其他计算机，选择“开始”|“运行”命令，出现如图 4-31 所示的窗口。

（5）在“打开”文本框中输入命令“ping 192.168.1.1 –t”，然后单击“确定”按钮，出现如图 4-32 所示。

（6）可以看出通过 Ping 的方式可以探测其他主机，此时将第（4）步骤的“通行”修改为“拦截”并保存刚才设置的规则，然后再次用 Ping 的方法来探测其他主机，得到如图 4-33 所示的结果，说明已经不能运用 Ping 的方式来探测其他主机了。



图 4-31 运行对话框

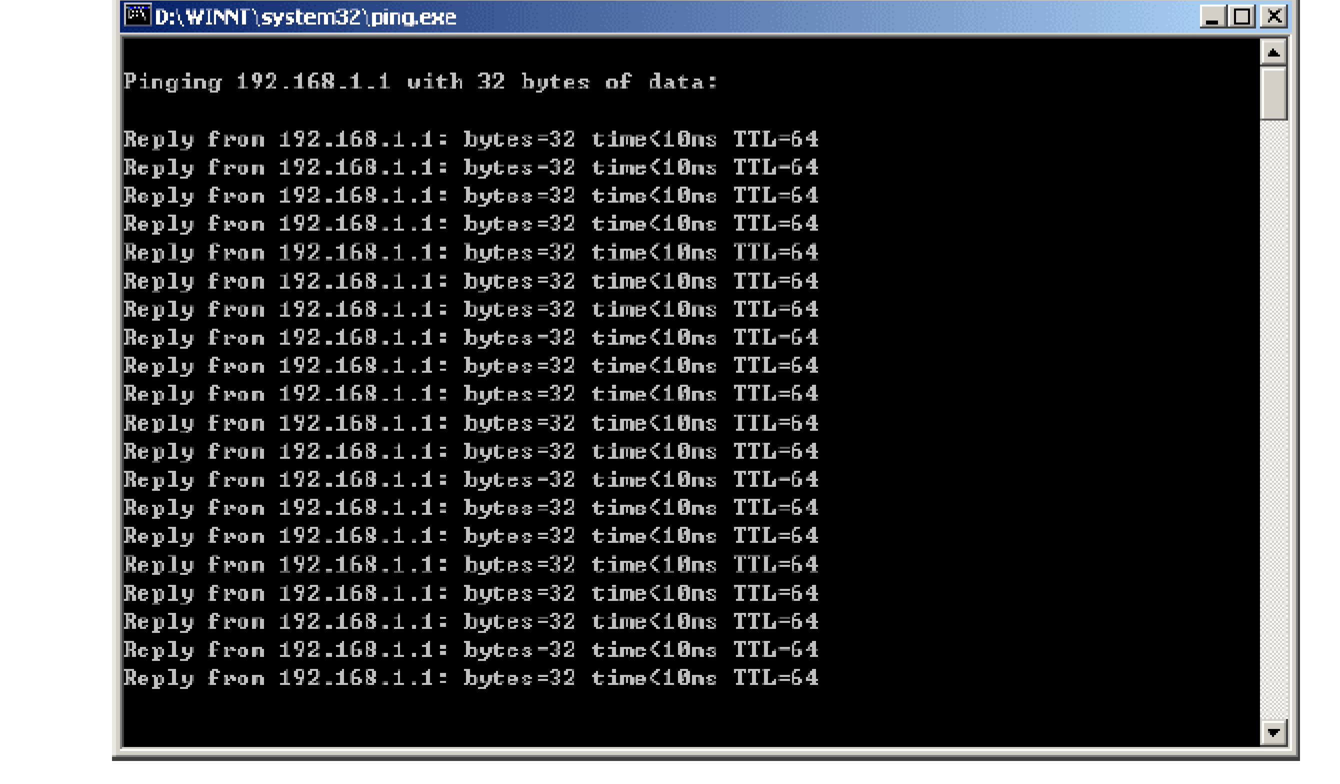


图 4-32 通过 Ping 探测其他主机

（7）“IP 管理规则”窗口上还提供有对 IP 管理规则的删除、添加、保存、导入、导出、上移、下移、清空等功能，可以根据实际需要对这些规则进行灵活设置。

系统设置的具体操作如下。

（1）选择“开始”|“程序”|“天网防火墙”|“天网防火墙”命令，出现“天网防火墙个人版”窗口，如图 4-25 所示。

（2）在“天网防火墙”窗口上单击“系统设置”按钮，出现如图 4-34 所示窗口。

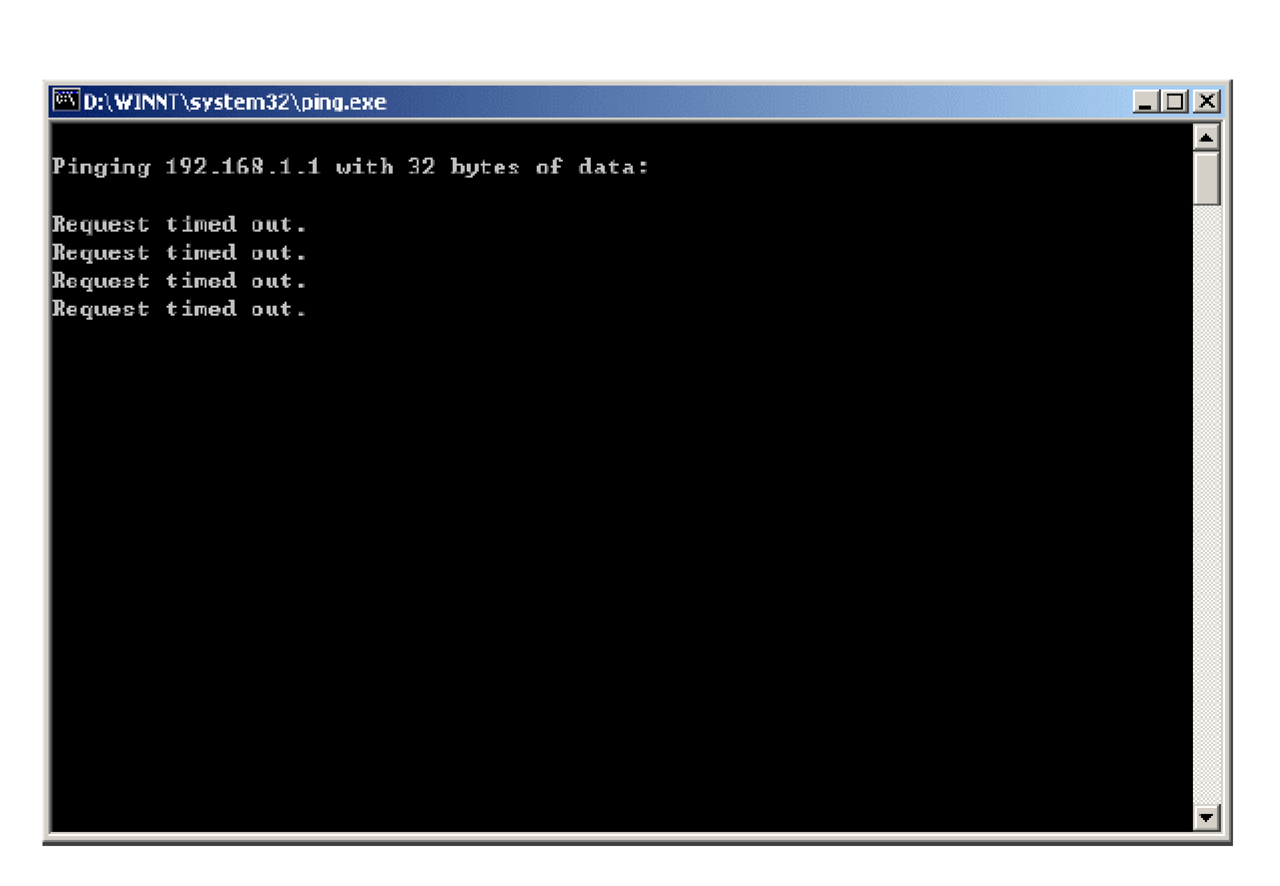


图 4-33 禁止用 Ping 探测其他主机



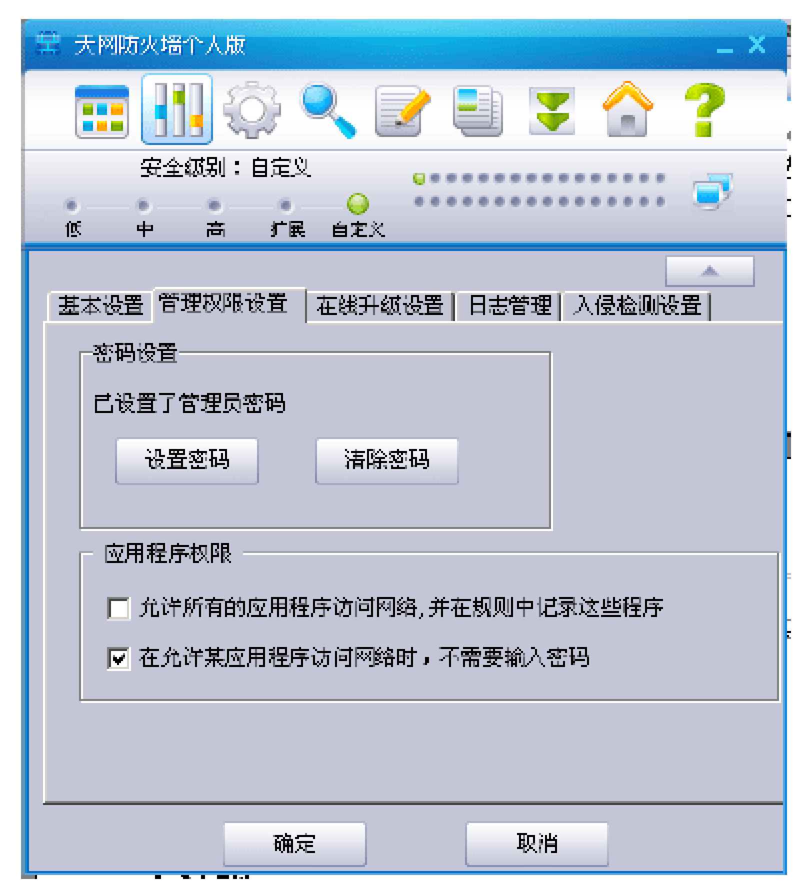
图 4-34 系统设置窗口

（3）系统设置窗口中包括多个选项卡，在基本设置选项卡中选择“开机后自动启动防火墙”单选框，计算机启动时，防火墙会随着计算机自动启动，如果没有选择这项，计算机启动以后需要手动启动防火墙。

（4）选择“管理权限设置”选项卡，可以进行密码设置以及防火墙的管理方式，如图 4-35 所示。

（5）单击“设置密码”按钮，可以设置管理密码，单击“清除密码”，可以清除以前的密码设置，还可以设置在运行应用程序通信时，是否需要输入密码。

（6）选择“在线升级设置”选项卡，这里可以设置升级策略，即是否在有升级的时候进行提示，如图 4-36 所示。



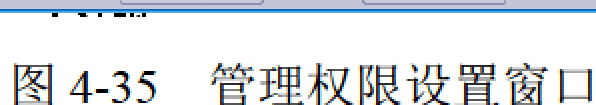


图 4-35　管理权限设置窗口

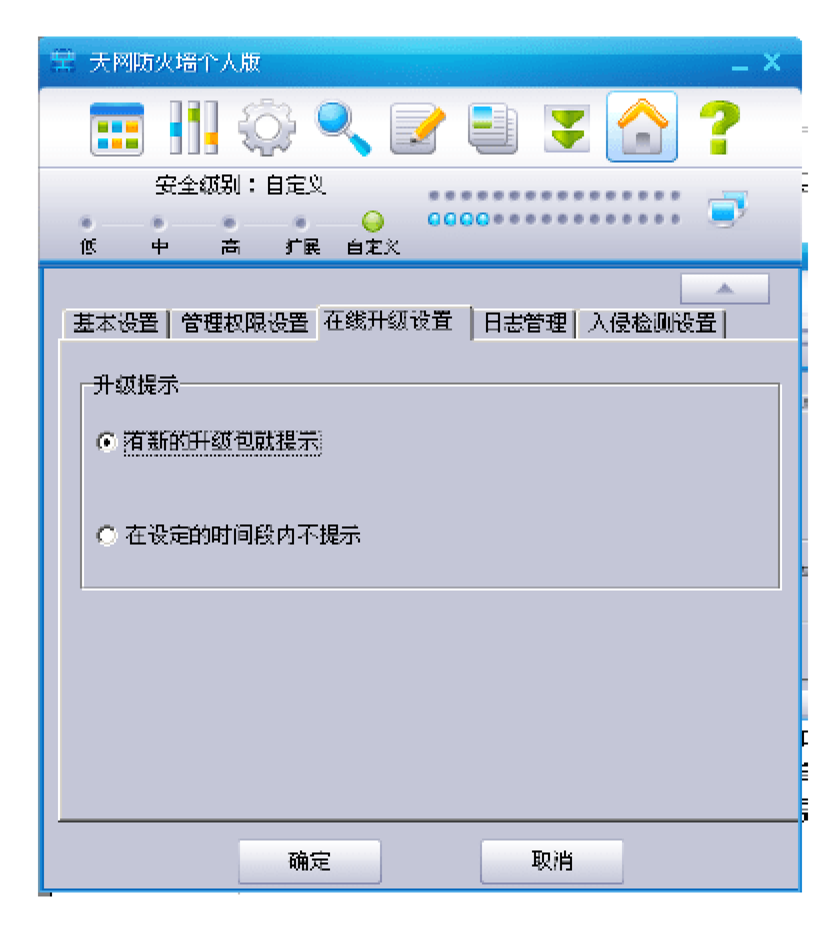


图 4-36　在线升级设置窗口

（7）选择“日志管理”选项卡，可以设置系统的日志管理方式，比如是否自动保存日志、保存日志的位置以及日志文件的大小限制等，如图 4-37 所示。

（8）选择“入侵检测设置”选项卡，可以进行简单的入侵检测设置，包括是否启动入侵检测功能、对检测到的入侵行为的处理方式，如图 4-38 所示。

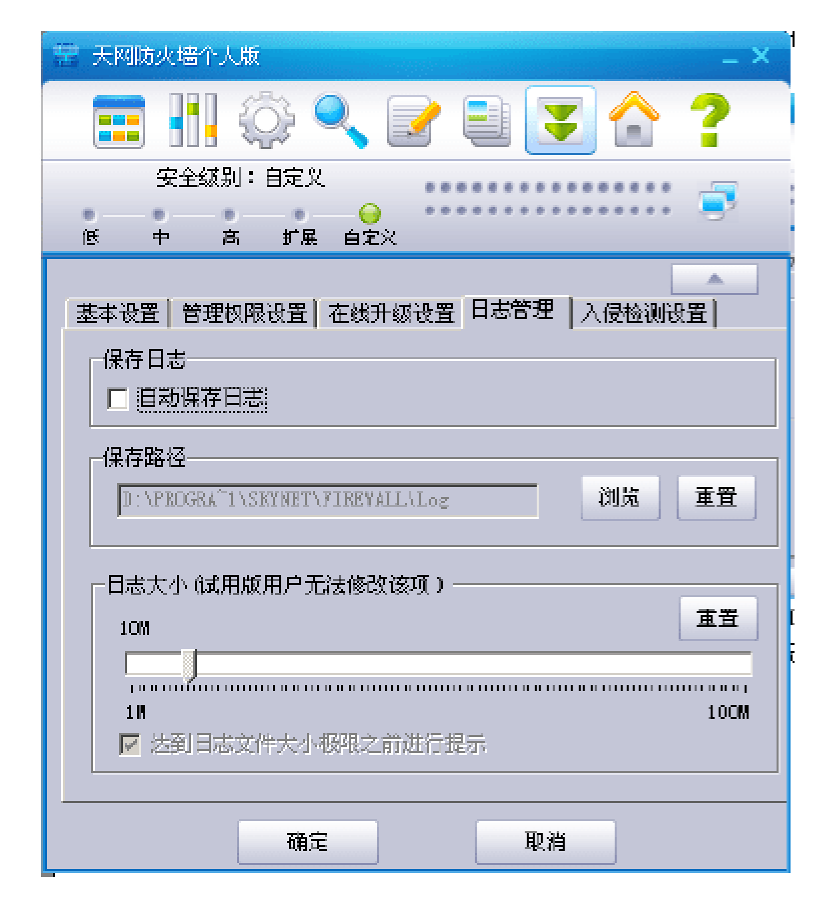


图 4-37　日志管理设置窗口

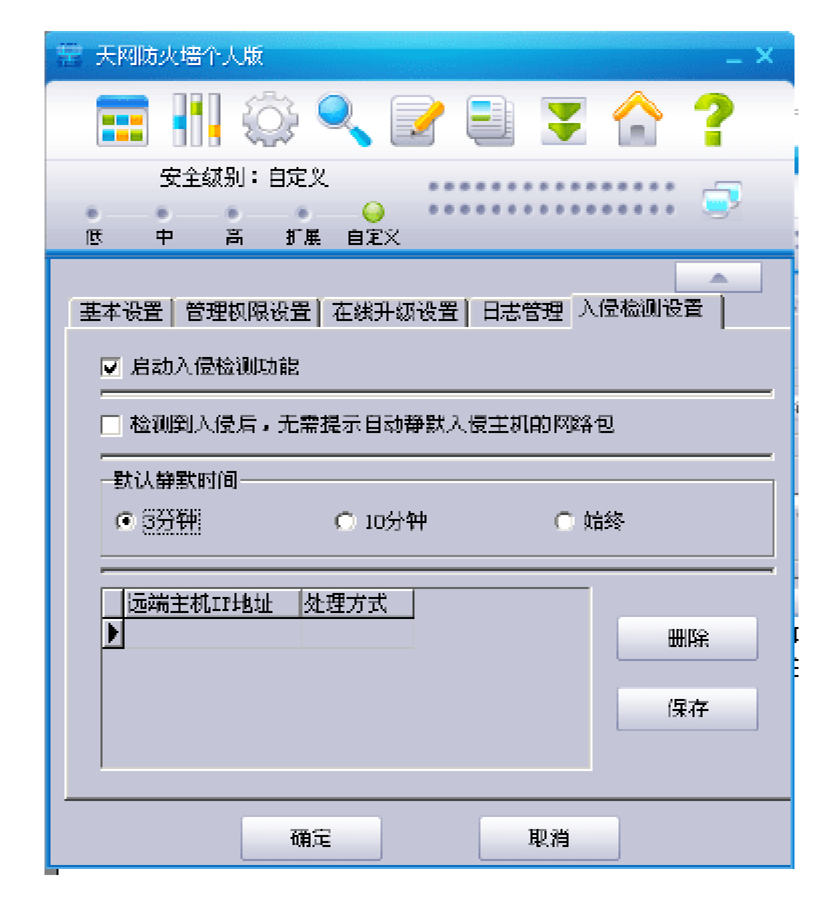


图 4-38　入侵检测设置窗口

（9）通过对上述的各种设置的了解，就可以更加灵活地使用防火墙来保护自己计算机系统的安全了。

习题

1．简述防火墙的功能。
2．如何对防火墙技术进行分类，各类技术的工作原理是什么？
3．防火墙体系结构包括哪些内容？
4．简述防火墙技术未来的发展趋势。
5．使用 IRIS 协议分析工具分析收发电子邮件过程。

第 5 章　计算机安全管理

教学提示

计算机安全管理主要对计算机系统存在的各种安全威胁进行管理。计算机是计算机网络中的一个重要组成部分，保证其安全对于整个网络的安全具有重要意义。

计算机安全管理涉及到硬件安全、操作系统安全、应用软件安全以及数据安全等多个方面，其中操作系统安全和数据安全具有非常重要的地位，操作系统安全是基础，数据安全是目的，唯有这二者同时得到保障，计算机的功能才能得以发挥。本章将对计算机操作系统安全和数据安全可能遇到的各种安全威胁进行探讨，并对其产生的原因、导致的危害以及解决方法进行说明。

通过对本章的学习，应当充分掌握计算机面临的各种安全威胁，理解其产生的原因、造成的危害以及解决的方法。计算机安全管理是一个复杂的系统工程，涉及的内容多而且复杂，同时随着时间的推移，新的内容还会不断加入进来，要做好这项工作，需要长期不断地归纳总结经验，不断提高分析问题和解决问题的能力。

教学重点

- 计算机安全管理的内容。
- 操作系统补丁。
- 系统安全配置。
- 系统备份。
- 数据安全。

5.1　软件安全

这里的软件安全包括系统软件安全和应用软件安全，如果说计算机硬件是躯体的话，那么计算机软件就是灵魂。整个计算机系统的安全必然少不了计算机软件的安全。计算机软件包括系统软件和应用软件，下面我们将对这两种软件的安全威胁进行讲解。

5.1.1　系统补丁

我们每天使用的 Windows 操作系统是一个非常复杂的软件系统，因此它难免会存在许多的安全漏洞，这些漏洞会被病毒、木马、恶意脚本、黑客利用，从而严重影响计算机使用和网络的安全和畅通。微软公司会不断发布升级程序供用户安装。这些升级程序就是“系统补丁”，因此及时为 Windows 安装系统补丁是十分必要的。

1．Windows 系统补丁

微软发布的系统补丁有两种类型：Hotfix 和 Service Pack，下面介绍它们之间的区别和联系。

Hotfix 是微软针对某一个具体的系统漏洞或安全问题而发布的专门解决程序，Hotfix 的程序文件名有严格的规定，一般格式为“产品名-KBXXXXXX-处理器平台-语言版本.exe”。现举一个例子来详细说明：微软针对震荡波病毒而发布的 Hotfix 程序名为“Win2K-KB835732-X86-CHS.exe”，这个补丁是针对 Win2000 系统的，其知识库编号为 835732，应用于 X86 处理器平台，语言版本为简体中文。

Hotfix 是针对某一个具体问题而发布的解决程序，因此它会经常发布，数量非常大。用户想要知道目前已经发布了哪些 Hotfix 程序是一件非常麻烦的事，更别提自己是否已经安装了。因此微软将这些 Hotfix 补丁全部打包成一个程序提供给用户安装，这就是 Service Pack，简称 SP。Service Pack 包含了发布日期以前所有的 Hotfix 程序，因此只要安装了它，就可以保证自己不会漏掉一个 Hotfix 程序。而且发布时间晚的 Service Pack 程序会包含以前的 Service Pack，例如 SP3 会包含 SP1、SP2 的所有补丁。

2．更新安装补丁

根据计算机的使用环境和目的，可以分为两种情况，一是个人或者家庭使用，另一种是企业使用。这里我们讲解一下对于个人用户如何安装和更新补丁程序。

（1）手动安装

微软专门客户帮助和支持网站 http://support.microsoft.com 提供了大量技术文档、安全公告、补丁下载服务，经常访问该网站可及时获得相关信息。参见图 5-1。



图 5-1　微软客户帮助和支持网站

另外，各类安全网站、杀毒软件厂商网站经常会有安全警告，并提供相关的解决方案，当然也包含了各类补丁的下载连接。通过连接下载回补丁程序后，只需运行安装并按提示操作即可。

（2）在线更新

手动安装是比较麻烦的，而且你不知道系统到底需要哪些补丁，因此对于一般用户推荐采用在线自动更新的方式。以 Windows 2000 为例，操作步骤如下。

① 选择“开始”|“设置”|“控制面板”命令，打开控制面板窗口，如图 5-2 所示。

② 双击“自动更新”选项，出现“自动更新”对话框，如图 5-3 所示。

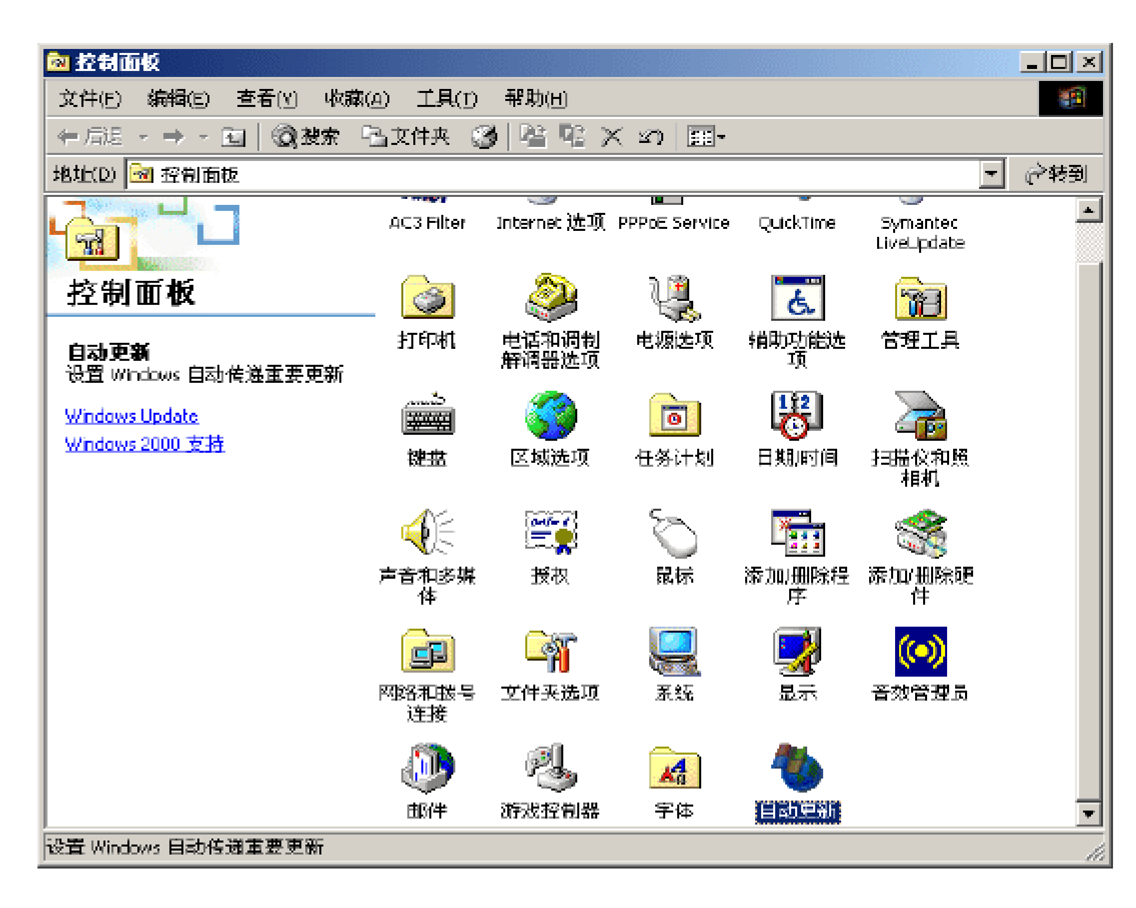


图 5-2　控制面板窗口中显示自动更新



图 5-3　自动更新对话框

③ 选择单选框“自动（推荐）”，并在下面的下拉列表框中选择自动下载更新的时间，可根据自己的实际需要来选择，一般选择休息时间，如图 5-3 设置的是每天 23:00 时进行自动更新，完成后点击确定，这样系统的自动更新功能就打开了，系统会在设定的时间自动连接微软网站下载更新，操作非常简单。

另外，我们还可以用如下方法更新。

（1）在 IE 浏览器中，选择“工具”| Windows Update 命令，或者选择“开始”| Windows Update 命令，IE 会自动打开 http://update.microsoft.com/windowsupdate，稍等一会儿后，IE 显示出更新方式选择页面。如图 5-4 所示。



图 5-4　选择更新方式页面

提示：有时，微软会先要求下载新的在线更新软件。

（2）可以看到，有快速和自定义两种升级方式，推荐一般用户选择“快速”方式，这种方式只查找安装最适合自己计算机最重要的更新程序。单击“快速”按钮后，IE 会自动查找最新的更新程序，如图 5-5 所示。

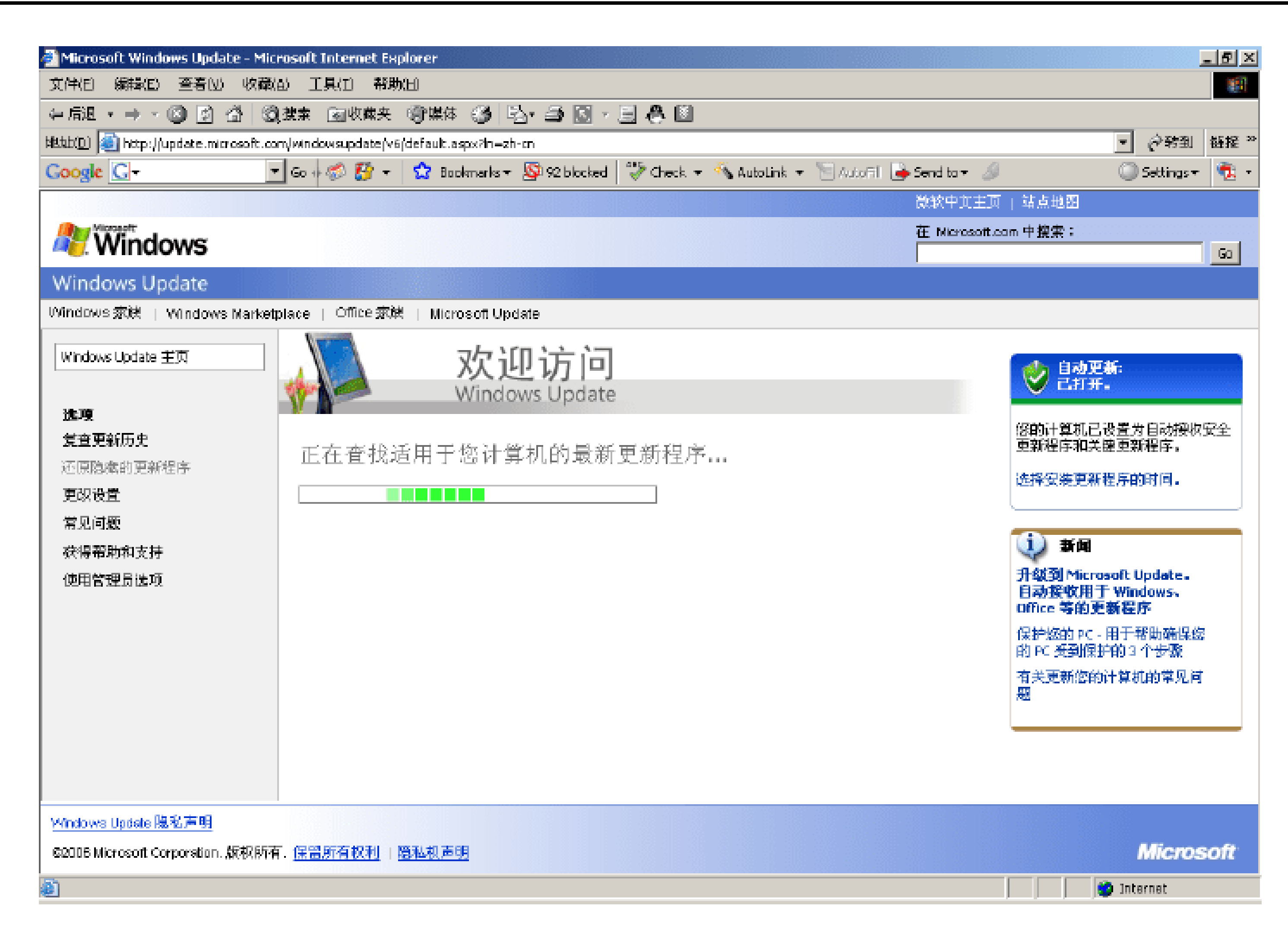


图 5-5　查找更新程序窗口

（3）查找最新的更新程序的窗口如图 5-6 所示。

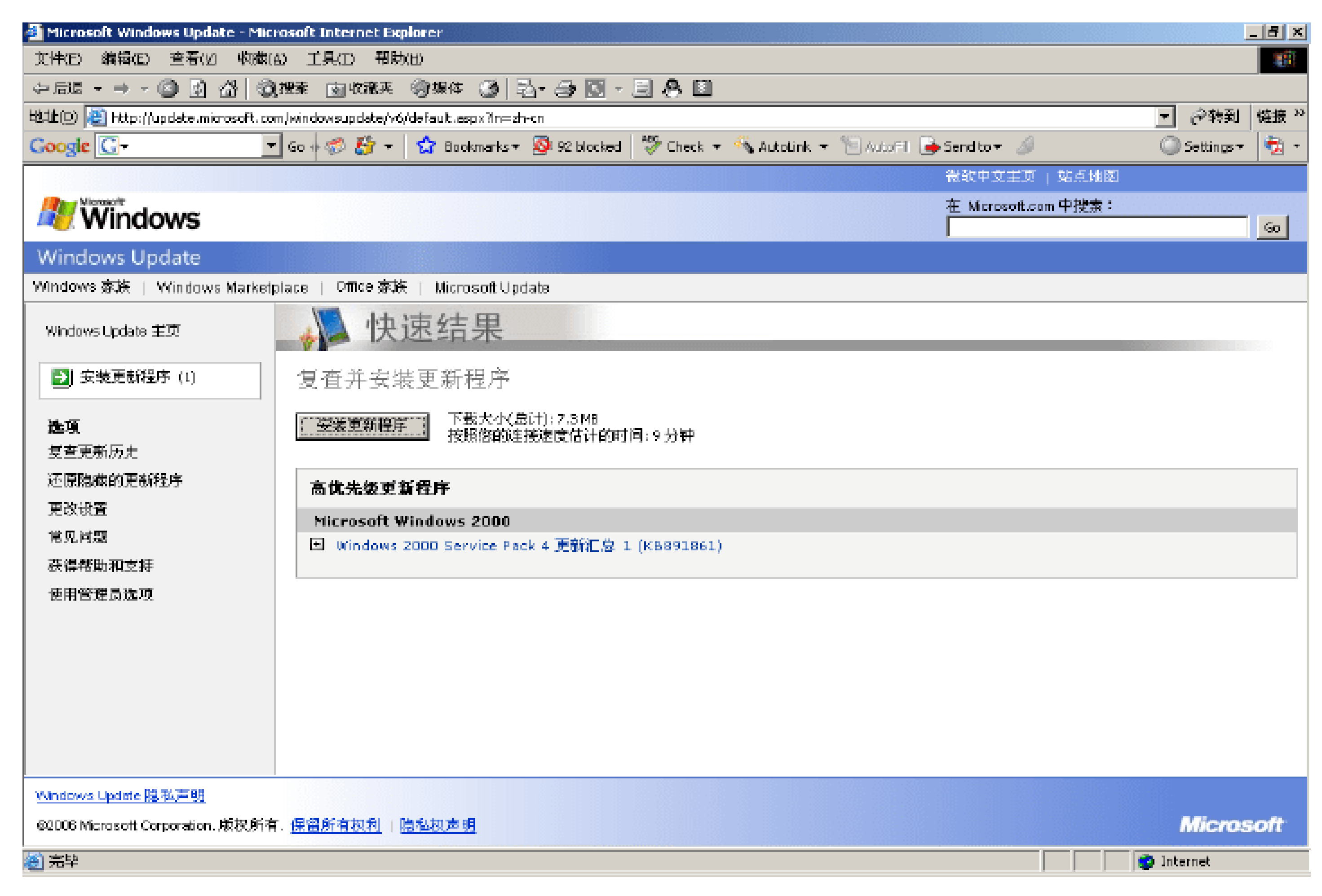


图 5-6　查找更新程序结果

（4）单击“安装更新程序”按钮，弹出对话框“正在安装更新程序”，如图 5-7 所示。

（5）更新程序安装完成后，显示如图 5-8 所示，此时可以单击“现在重启动”按钮来完成更新。



图 5-7　正在安全更新程序窗口



图 5-8　完成更新程序安装

> **提示：**有时系统有多个更新软件需要安装，而且有些更新软件需要重新启动计算机才能完成，所以可以重复上述步骤来完成。

3．查看已安装补丁

有时需要确定计算机系统是否安装了某个补丁，这时就需要知道计算机系统已经安装了哪些补丁，可以通过下列两种简单的方法来解决。

（1）通过注册表查看

当安装了系统补丁后，注册表中会留下相关信息，具体位置视操作系统的不同而异：

Windows 2000：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000

Windows XP：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP

Windows Server 2003：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows Server 2003

查看方法如下。

① 选择“开始”|“运行”命令，出现“运行”对话框，如图 5-9 所示。

② 在文本框中输入 regedit，然后单击“确定”按钮或者按回车键，出现注册表编辑器窗口，在其中找到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000 位置，如图 5-10 所示。

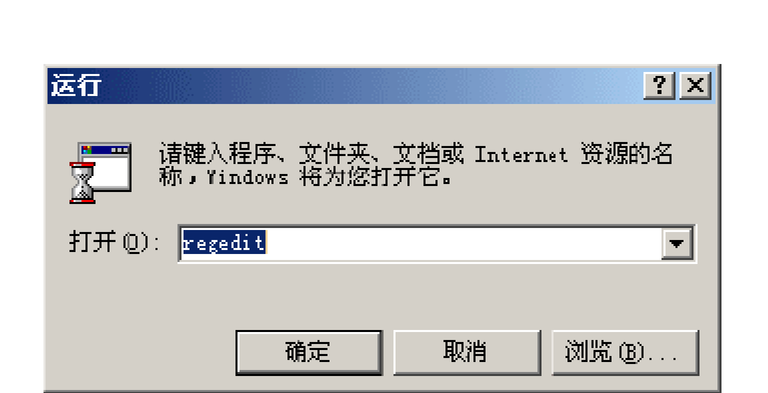


图 5-9　启动注册表

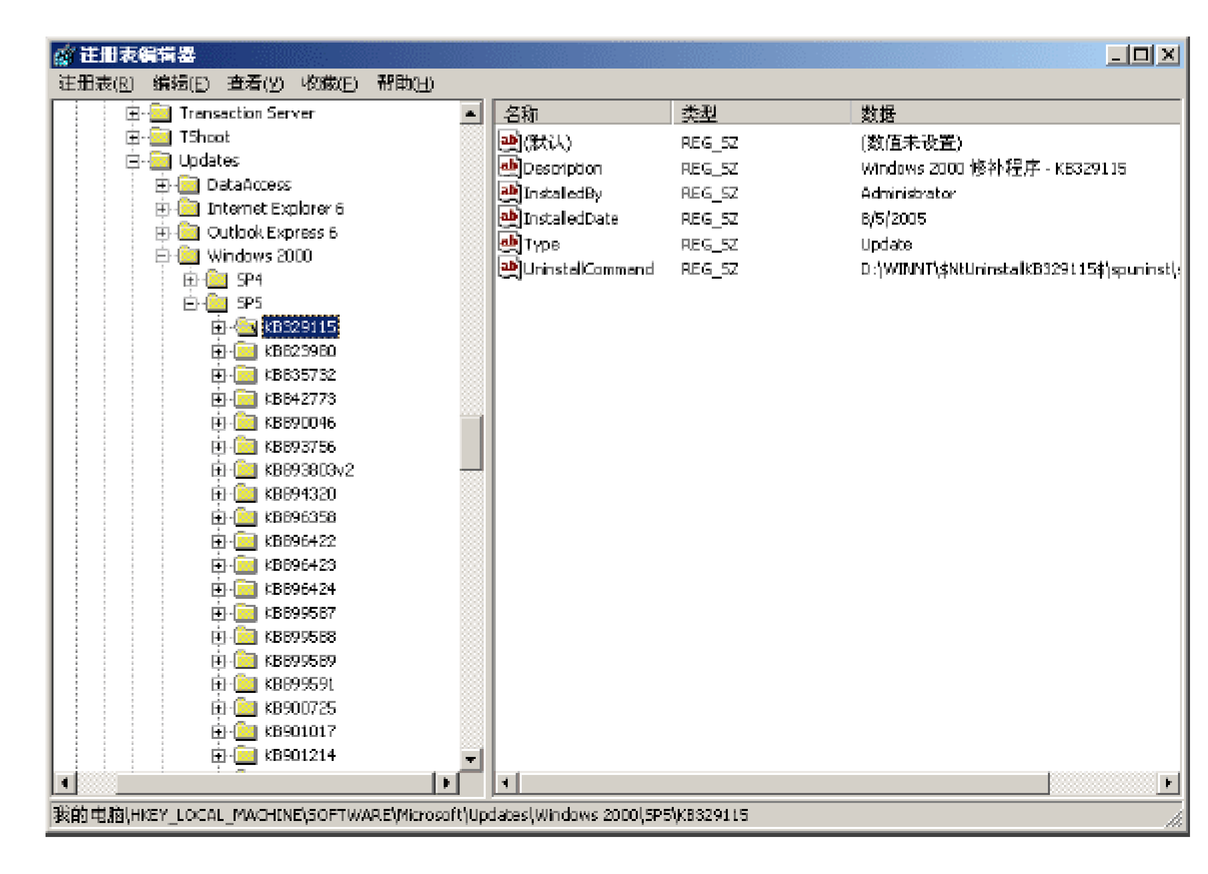


图 5-10　注册表中查看更新

③ 从“注册表编辑器”窗口中可以看到，Windows 2000 下面有 SP4 和 SP5 项目，双击 SP5，即可看到所安装的更新程序的名称，单击 KB329115，可在右边窗口中看到该补丁的相关信息，Description 项表示更新程序的描述，InstalledDate 项表示安装时间等，如图 5-11 所示。

（2）利用专用软件 WinUpdatesList

笔者推荐一款专门显示、管理系统补丁信息的工具软件——WinUpdatesList，该工具可以从网上免费下载。WinUpdatesList的主窗口如图 5-12 所示。

窗口中包含两个面板：上方的面板中显示所有已安装在你的计算机中的更新列表，列表显示了补丁名称、描述等详细信息。当你在上方的面板中选择一个 hotfix（类型为 Update）更新，下方的面板中将会显示选定 hotfix 安装的文件列表，如图 5-13 所示。

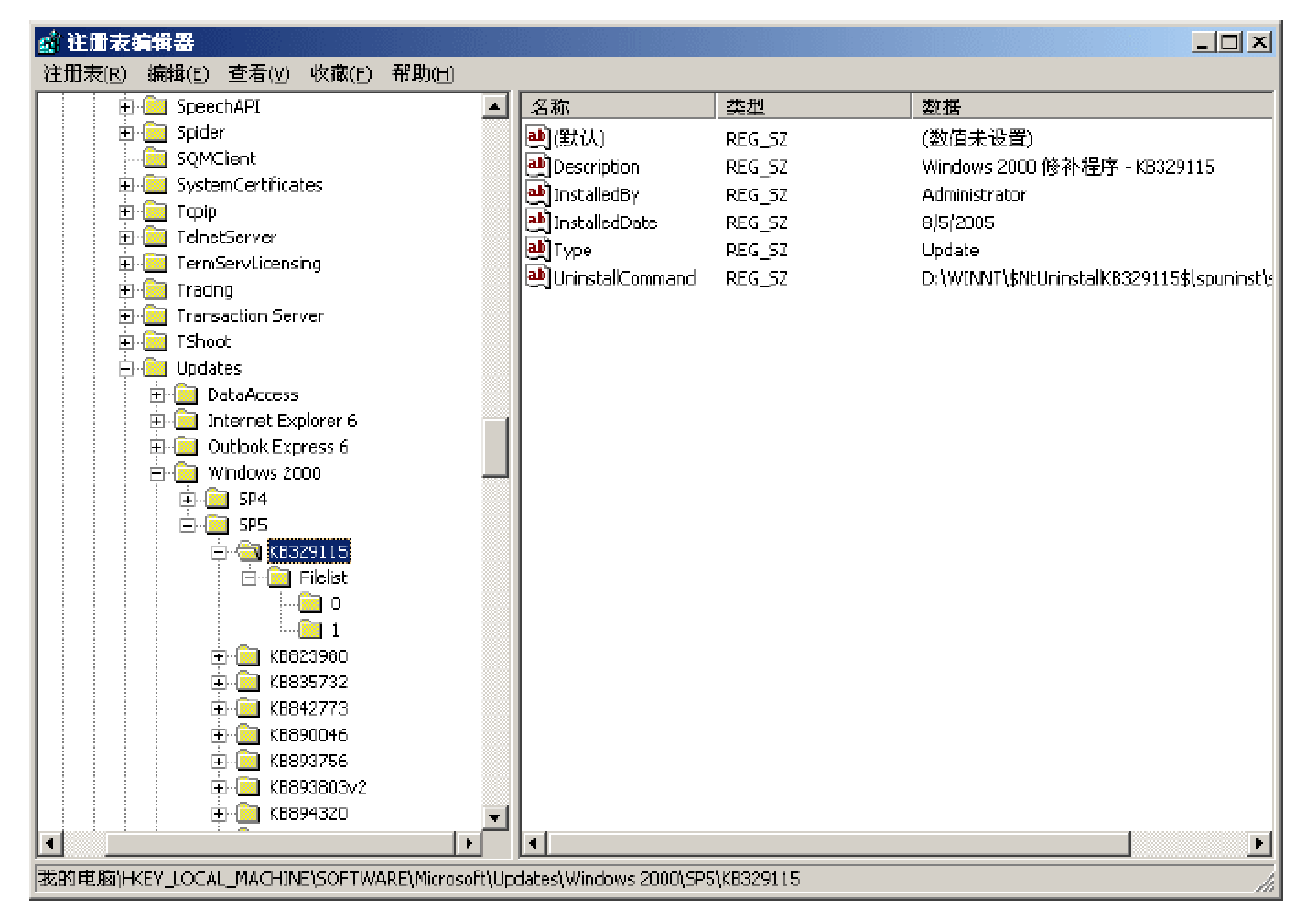


图 5-11　注册表中查看更新信息

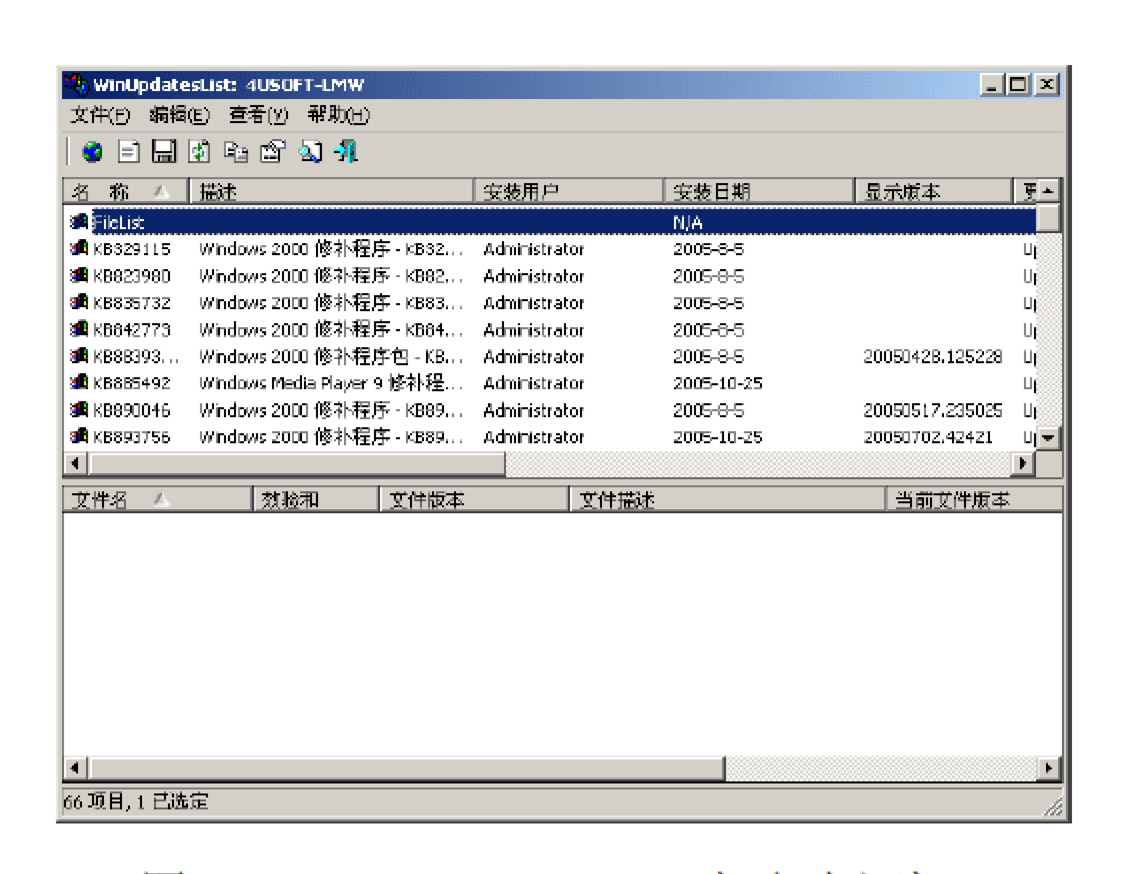


图 5-12　WinUpdatesList 启动时主窗口

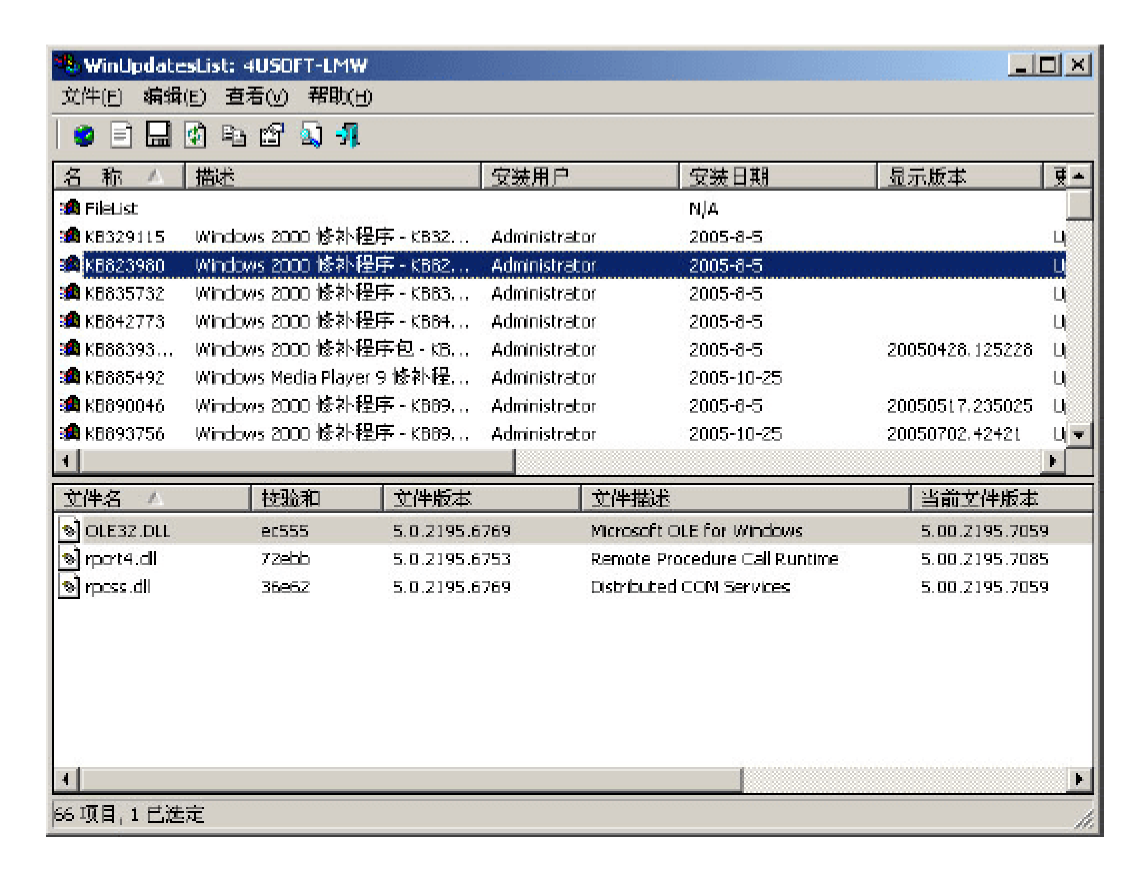


图 5-13　显示选定更新的文件列表

如果想要获得某个指定更新的详细信息，在上方的面板中选择希望查看的项目，然后在“文件”菜单（或者右键弹出菜单）中选择“打开网页连接”命令。浏览器会自动打开一个包含选定更新信息的微软站点的窗口，如图 5-14 所示，这样就可以了解这个升级包的所有信息了。

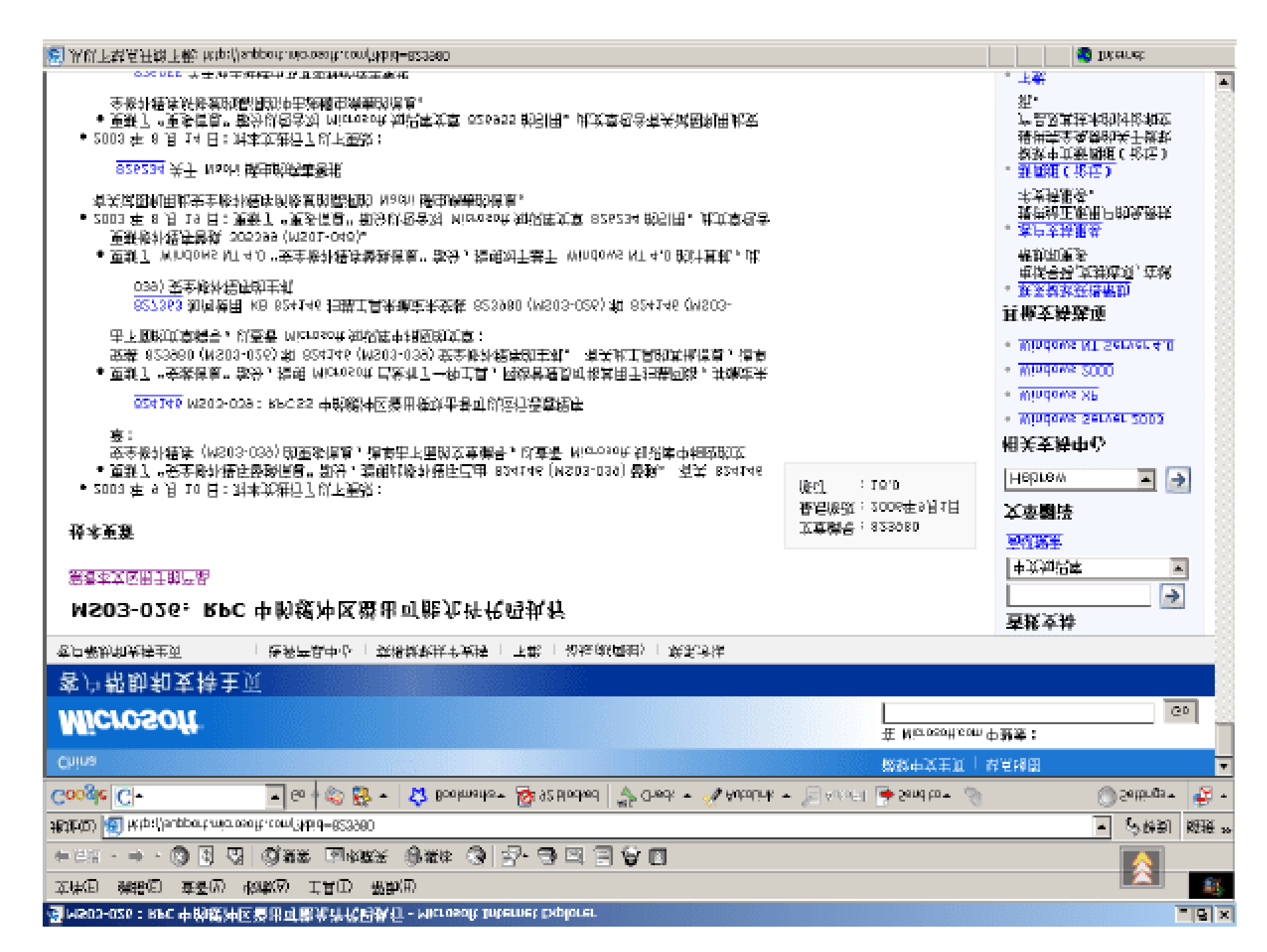


图 5-14　打开连接的网页窗口

> **提示：** 需要注意的是在 Windows 98/ME 的系统中，某些栏目可能无法被正常显示，这是因为相关的信息没有被保存在注册表中。

5.1.2 配置管理

计算机操作系统为了提供丰富、灵活的功能，以方便满足更多的客户需求，当然，也正是因为如此，操作系统提供了各种各样的参数配置，有时为了使用上的方便，有时为了使用上的安全，只有合理配置，才能满足其需求，相反地，如果没有对系统的各种参数合理配置，也会为系统带来安全隐患。

没有经过合理配置的计算机，在使用过程中容易出现安全问题，尤其是连接到网络时更容易受到来自网络的攻击，主要包括以下几个方面。

（1）被他人盗取密码；

（2）系统被木马攻击；

（3）浏览网页时被恶意的 java scrpit 程序攻击；

（4）QQ 被攻击或泄露信息；

（5）病毒感染；

（6）系统存在漏洞使他人攻击自己；

（7）黑客的恶意攻击。

1. 察看本地共享资源

查看本地资源的操作步骤如下。

（1）选择“开始”|“运行”命令，出现“运行”对话框。输入 CMD 并回车，如图 5-15 所示。

（2）在随后出现的 CMD 窗口中，输入 net share 并回车。可以看到，本机上的共享名称、资源以及注释说明，如图 5-16 所示。



图 5-15　启动命令行程序

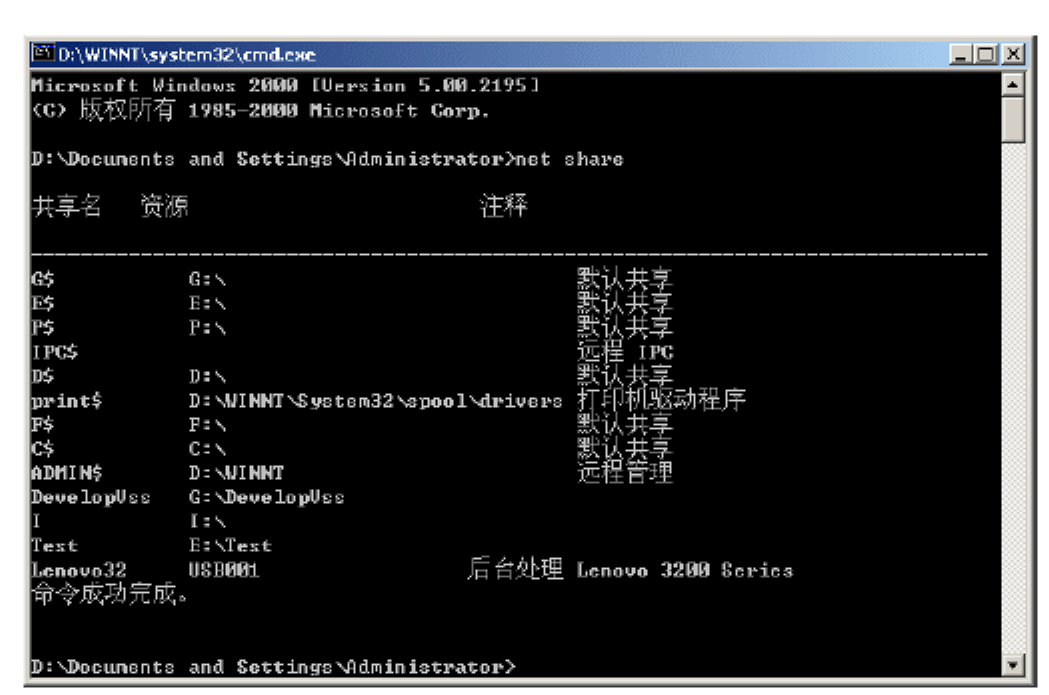


图 5-16　启动命令行程序

2. 删除默认共享

如果看到有异常共享，那么应该关闭，也就是删除。

> **提示：** 有时你关闭共享下次开机的时候又出现了，就应该考虑一下，机器是否已经被黑客所控制了，或者中了病毒。

删除默认共享的命令如下。

net share 共享名 /delete

下面是删除共享的例子：

net share admin$ /delete　　　删除 admin$共享

net share c$ /delete　　　　删除 c$

net share d$ /delete　　　　删除 d$

3．删除 ipc$空连接

删除 ipc$空连接需要在注册表中进行。方法如下：

（1）选择“开始”|“运行”命令，出现“运行”对话框。

（2）输入 regedit，出现“注册表编辑器”窗口。在注册表中找到 HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControSet\Control\LSA 项，如图 5-17 所示。

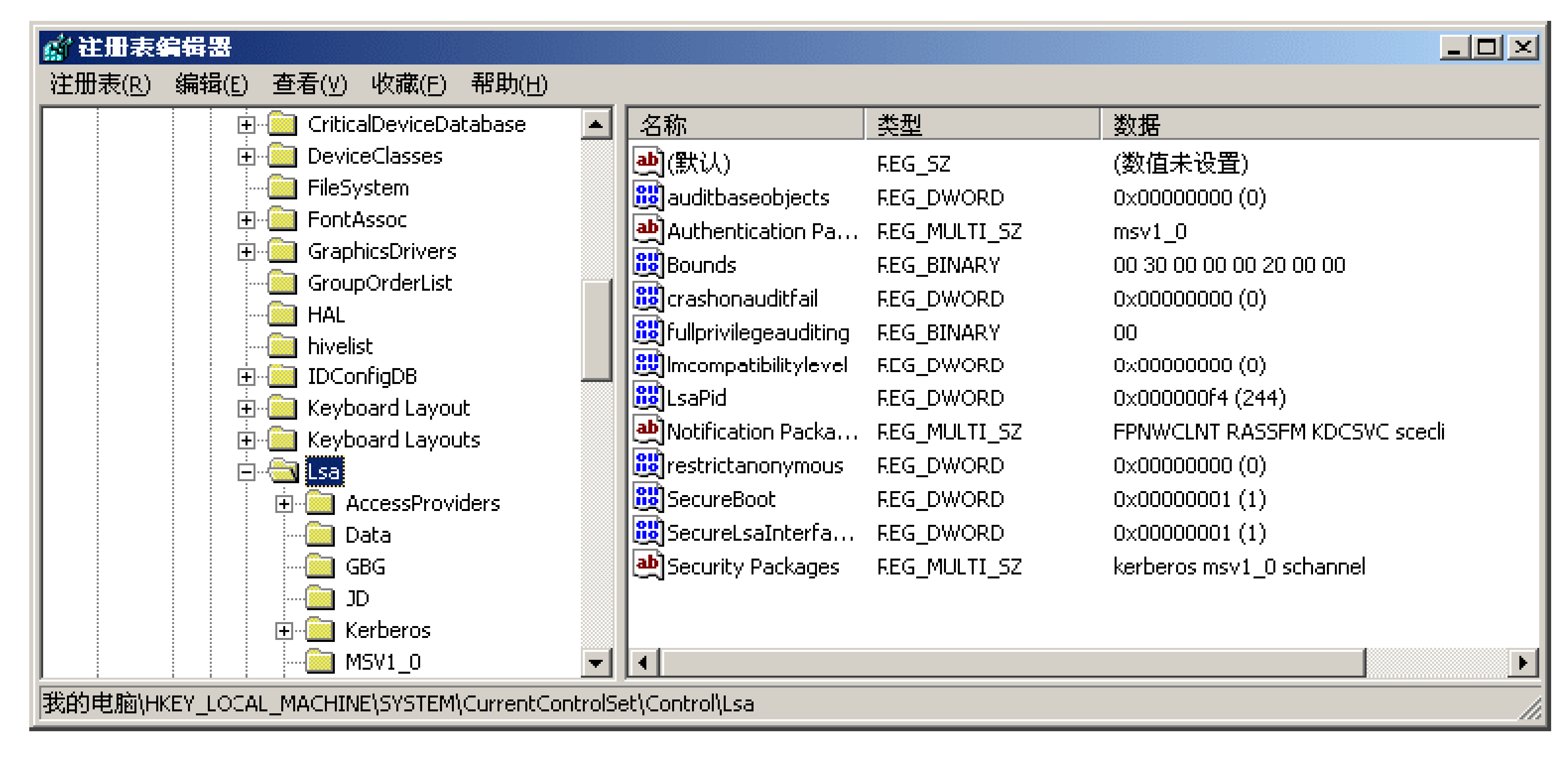


图 5-17　“注册表编辑器”窗口

（3）双击 RestrictAnonymous，出现“编辑双字节值”对话框，将“数值数据”由 0 改为 1，如图 5-18 所示。

（4）单击“确定”按钮。

4．关闭 139 端口

操作步骤如下。

（1）选择“开始”|“设置”|“网络和拨号连接”命令，出现“网络和拨号连接”窗口，如图 5-19 所示。



图 5-18　修改注册表键值窗口



图 5-19　网络和拨号连接窗口

（2）双击“本地连接”，出现“本地连接 状态”对话框，如图 5-20 所示。

（3）单击“属性”按钮，出现“本地连接 属性”对话框，如图 5-21 所示。





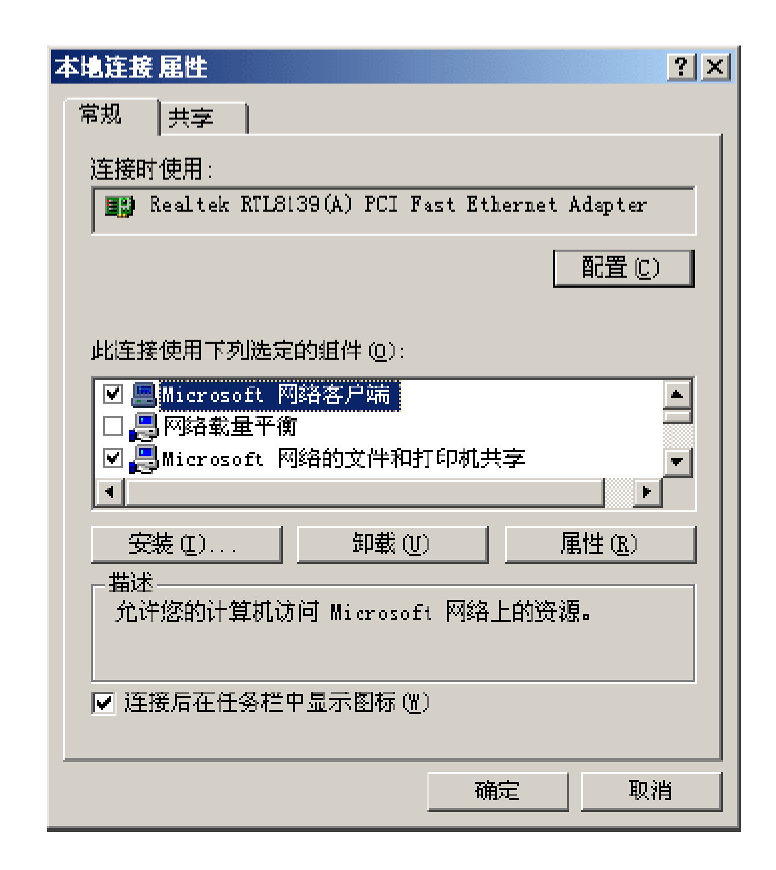
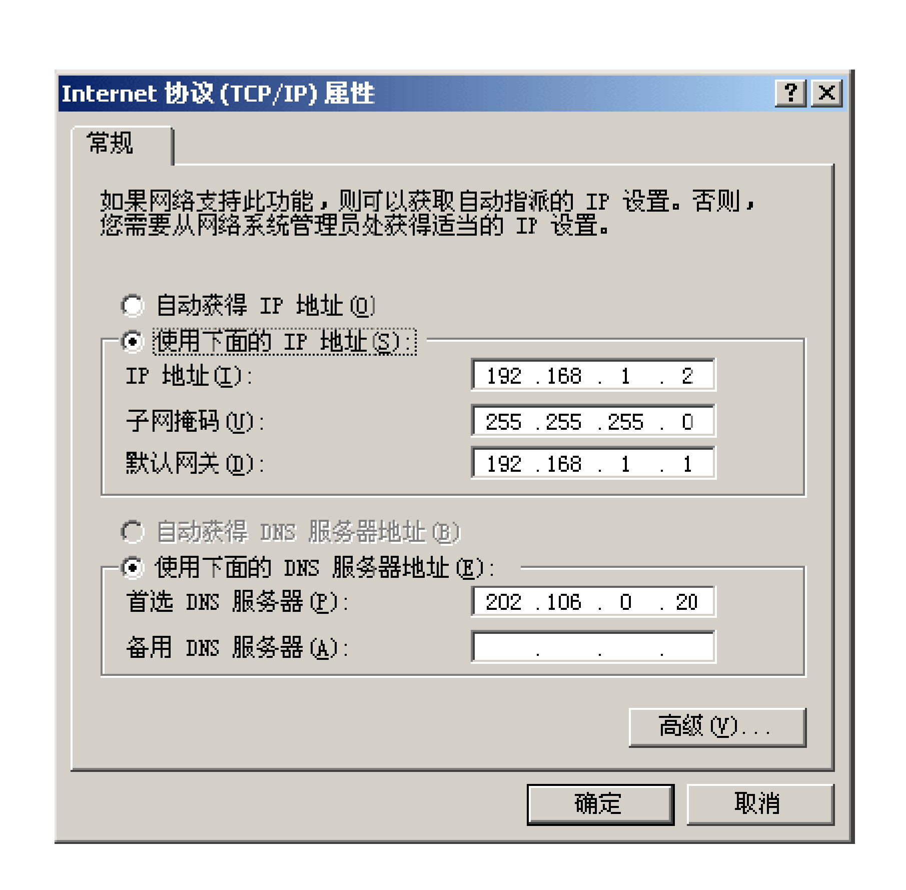


图 5-20　本地连接状态对话框　　　　图 5-21　本地连接属性对话框

（4）在“此连接使用下列选定的组件”列表中选择“Microsoft 网络客户端”项，并双击，出现“Internet 协议（TCP/IP）属性”对话框，如图 5-22 所示。

（5）单击“高级”按钮，出现“高级 TCP/IP 设置”对话框，并选择“WINS”选项卡，如图 5-23 所示。



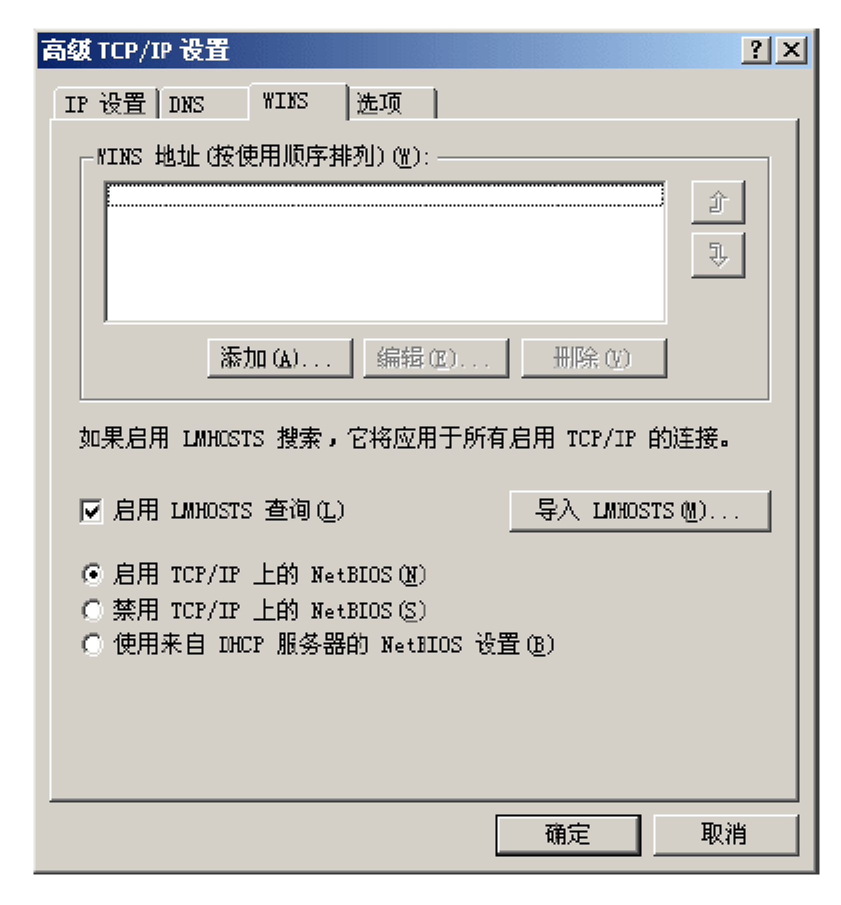


图 5-22　Internet 协议（TCP/IP）属性对话框　　　　图 5-23　WINS 选项卡窗口

（6）选择“禁用 TCP/IP 上的 NetBIOS”单选按钮，然后单击“确定”按钮，139 端口就成功关闭了。

5．防止 rpc 漏洞

操作步骤如下。

（1）选择“开始”|“设置”|“控制面板”命令，出现“控制面板”窗口，如图 5-2 所示。

（2）在“控制面板”中双击“管理工具”，出现“管理工具”窗口，如图 5-24 所示。

（3）在管理工具窗口中，双击“服务”，出现“服务”窗口，如图 5-25 所示。

（4）找到“Remote Procedure Call (RPC) Locator”服务并双击，出现“Remote Procedure Call (RPC) Locator 的属性（本地计算机）”对话框，并选择“故障恢复”选项卡，如图 5-26 所示。

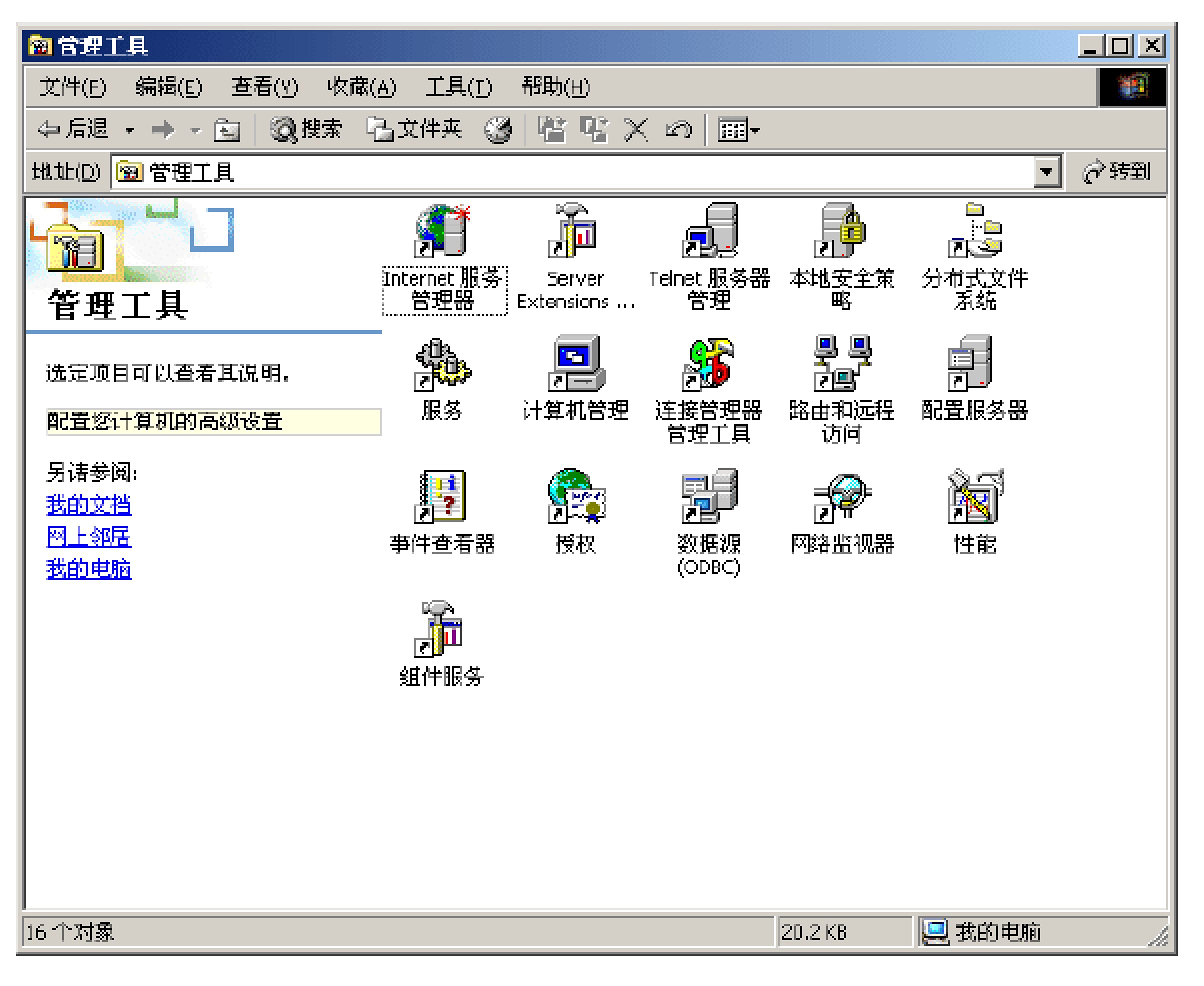


图 5-24　管理工具窗口

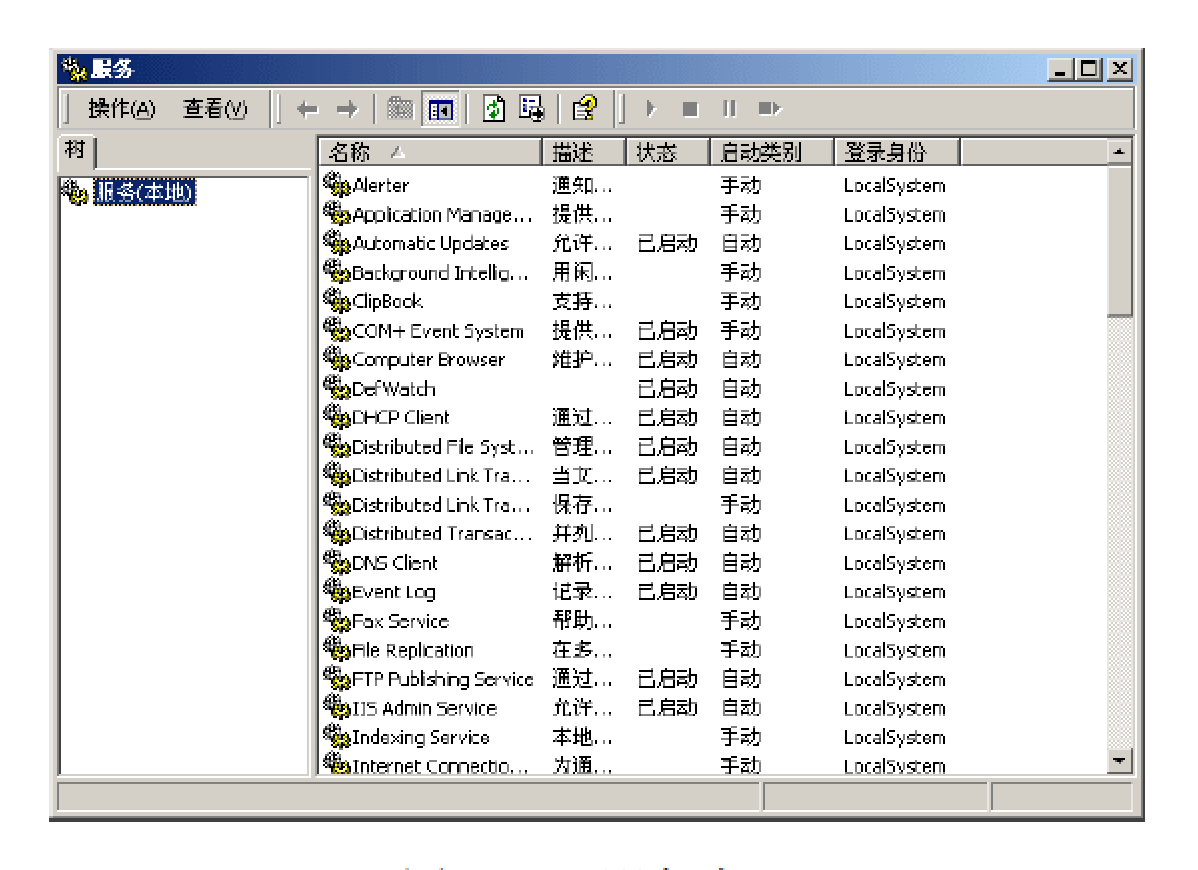






图 5-25　服务窗口　　　　图 5-26　服务属性对话框

（5）将“第一次失败”下拉列表，“第二次失败”下拉列表，“后续失败”下拉列表，都选择“不操作”，然后单击“确定”按钮，防止 rpc 漏洞的操作就完成了。

6．关闭 445 端口

关闭该端口的操作步骤如下。

（1）选择“开始”|“运行”命令，出现“运行”对话框，输入 regedit，并按回车键。

（2）在打开的“注册表编辑器”窗口左边列表中选择 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters，再在右侧窗口中，单击右键，在弹出的菜单中选择“新建”|“双字节值”菜单项，新建一个键值项，如图 5-27 所示。

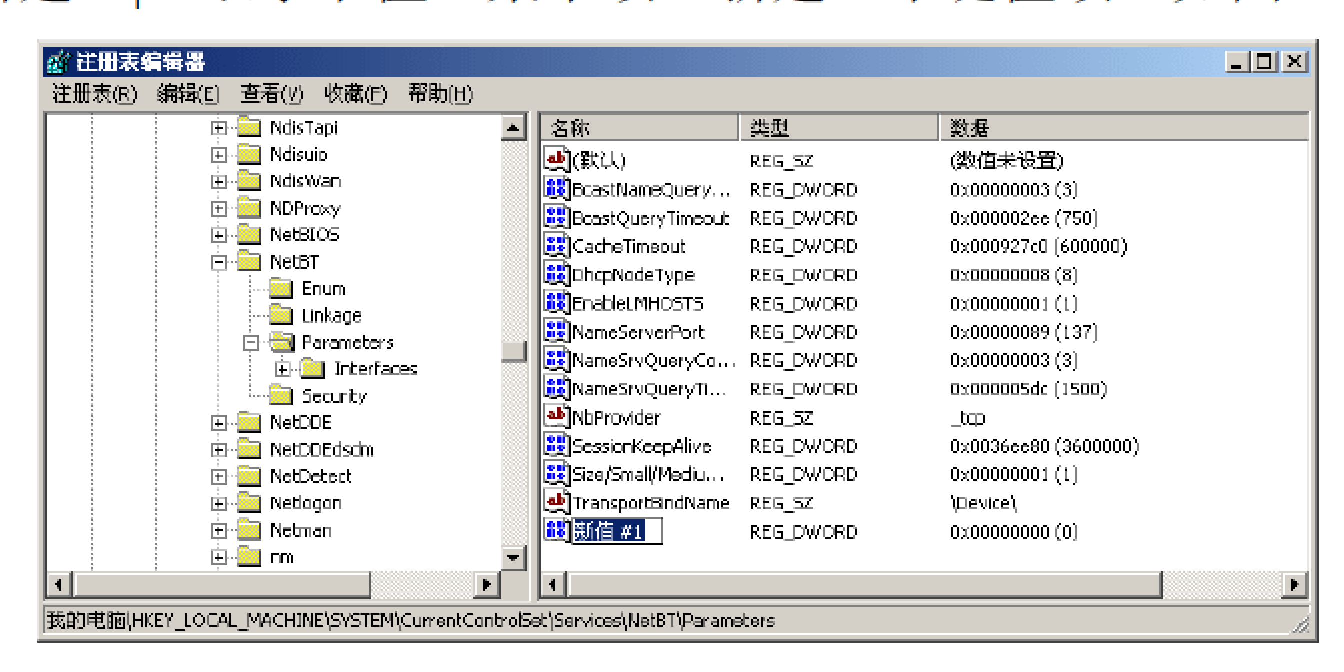


图 5-27　新建键值项

（3）右键单击“新值 #1”，选择“重命名”命令，将键值名改为 SMBDeviceEnabled，默认值为 0，和需要设置的值一致，这样就完成 445 端口关闭了。

7. 关闭 3389 端口

Windows 2000 Server 系统下关闭该端口的操作步骤如下。

（1）选择“开始”|“程序”|“管理工具”|“服务”命令，出现“服务”窗口，在服务列表中找到“Terminal Services”服务并双击，出现“Terminal Services 的属性（本地计算机）”对话框，如图 5-28 所示。

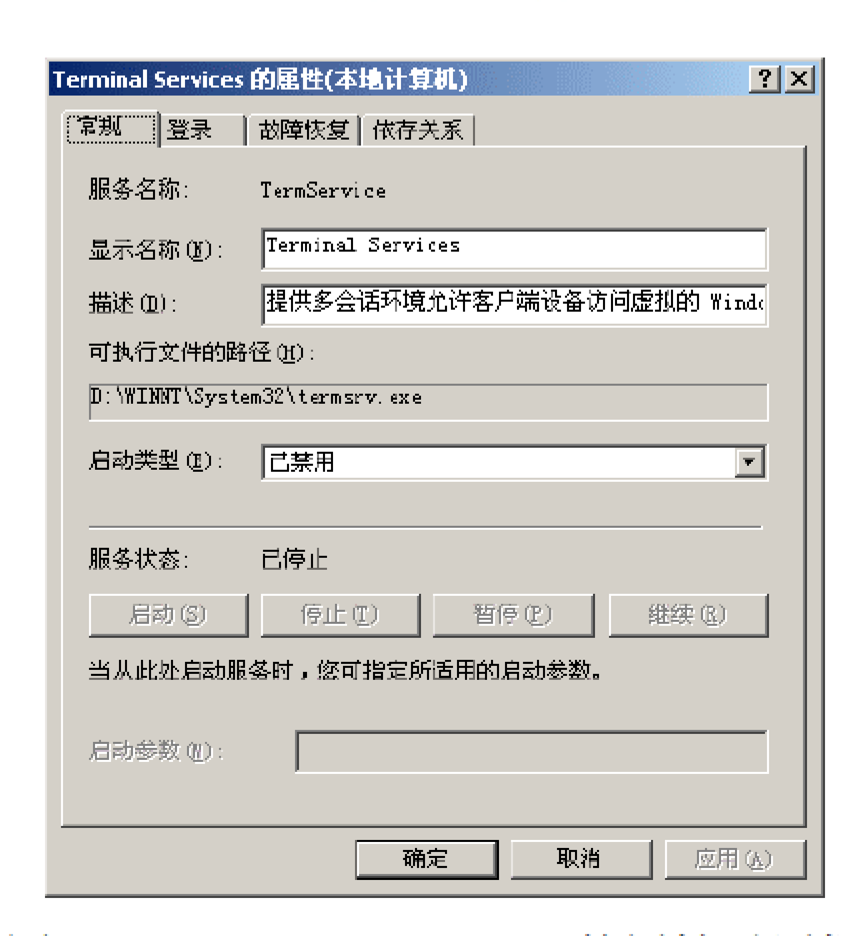
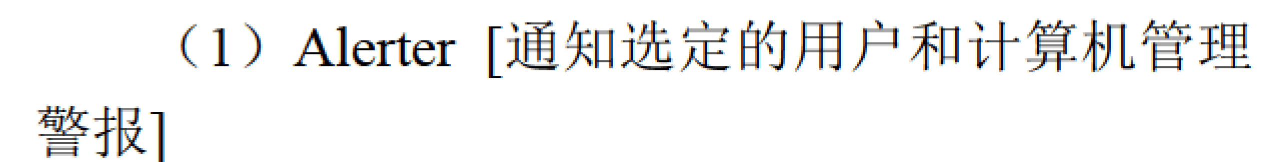


图 5-28　Terminal Services 的属性对话框

（2）在“启动类型”下拉列表框中选择“手动”选项，单击“停止”按钮，并单击“确定”按钮，完成 3389 端口的关闭。

8. 禁用服务

操作方法和关闭 3389 端口的方法基本上是一样的，所以此处不再一一详细讲解，下面将一些服务的名称和功能列举出来，根据自己的实际需要，可以选择性地禁用这些服务。



（1）Alerter [通知选定的用户和计算机管理警报]

（2）ClipBook [启用“剪贴簿查看器”储存信息并与远程计算机共享]

（3）Distributed File System [将分散的文件共享合并成一个逻辑名称，共享出去，关闭后远程计算机无法访问共享]

（4）Distributed Link Tracking Server [适用局域网分布式链接跟踪客户端服务]

（5）Human Interface Device Access [启用对人体学接口设备(HID)的通用输入访问]

（6）IMAPI CD-Burning COM Service [管理 CD 录制]

（7）Indexing Service [提供本地或远程计算机上文件的索引内容和属性，泄露信息]

（8）Kerberos Key Distribution Center [授权协议登录网络]

（9）License Logging [监视 IIS 和 SQL 如果你没安装 IIS 和 SQL 的话就停止]

（10）Messenger [警报]

（11）NetMeeting Remote Desktop Sharing [Netmeeting 公司留下的客户信息收集]

（12）Network DDE [为在同一台计算机或不同计算机上运行的程序提供动态数据交换]

（13）Network DDE DSDM [管理动态数据交换（DDE）网络共享]

（14）Print Spooler [打印机服务，没有打印机就禁止吧]

（15）Remote Desktop Help Session Manager [管理并控制远程协助]

（16）Remote Registry [使远程计算机用户修改本地注册表]

（17）Routing and Remote Access [在局域网和广域网提供路由服务，黑客通过路由服务刺探注册信息]

（18）Server [支持此计算机通过网络的文件、打印和命名管道共享]

（19）Special Administration Console Helper [允许管理员使用紧急管理服务远程访问命

令行提示符]

（20）TCP/IPNetBIOS Helper [提供 TCP/IP 服务上的 NetBIOS 和网络上客户端的 NetBIOS 名称解析的支持而使用户能够共享文件、打印和登录到网络]

（21）Telnet [允许远程用户登录到此计算机并运行程序]

（22）Terminal Services [允许用户以交互方式连接到远程计算机]

（23）Window s Image Acquisition (WIA) [照相服务，应用与数码摄像机]

如果发现机器开启了一些很奇怪的服务，如 r_server 这样的服务，必须马上停止该服务，因为这完全有可能是黑客使用控制程序的服务端。

9．账号密码的安全原则

（1）首先禁用 Guest 账号，这是计算机最大的安全隐患之一。具体的操作方法如下。

① 选择“开始”|“程序”|“管理工具”|“计算机管理”命令，出现“计算机管理”窗口，如图 5-29 所示。

② 在“计算机管理”窗口左边，依次选择“系统工具”|“本地用户和组”|“用户”，然后在右边窗口中双击 Guest 项，出现“Guest 属性”对话框，如图 5-30 所示。

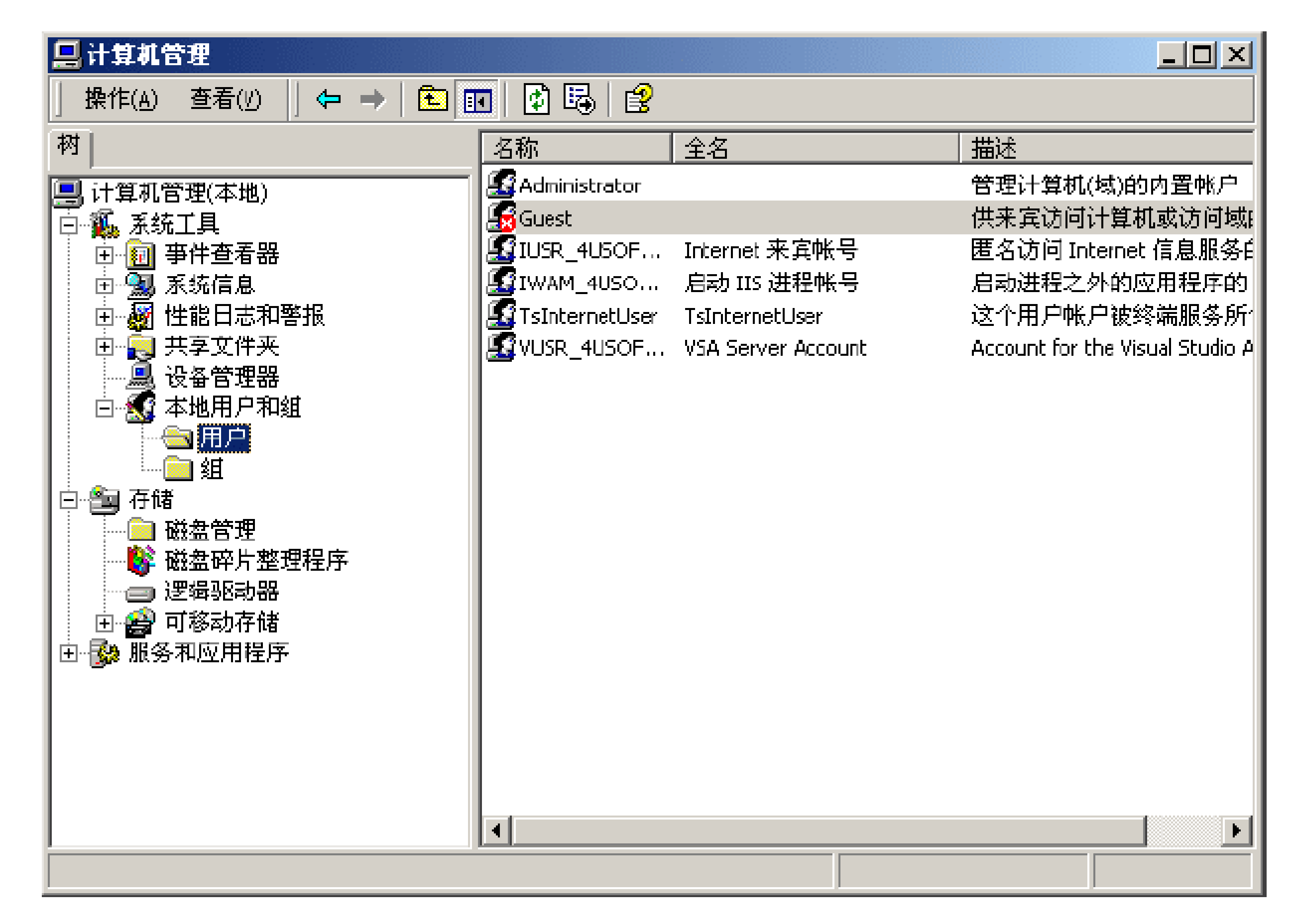


图 5-29　计算机管理窗口

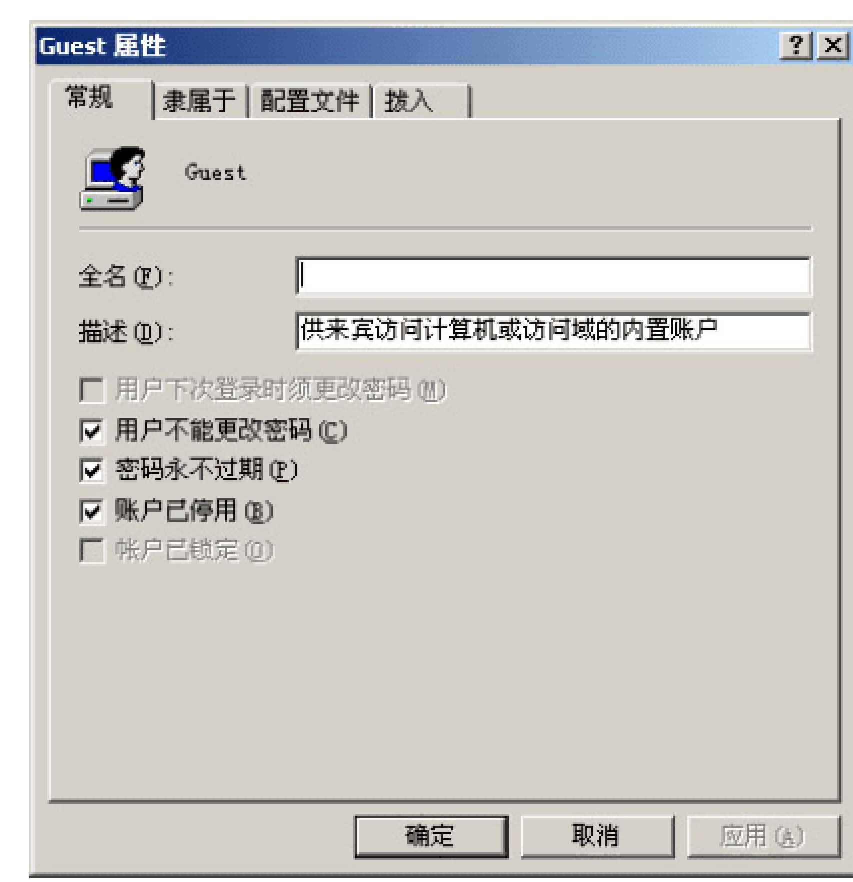


图 5-30　Guest 属性对话框

③ 选择“账户已停用”复选框，然后单击“确定”按钮，这样就禁止 Guest 账号了。

（2）为了提高系统的安全性，系统内建的 Administrator 账号可以改名，而且要设置一个密码，最好是 8 位以上字母数字符号组合。

修改系统管理员账号名称的具体操作如下。

① 选择“开始”|“程序”|“管理工具”|“本地安全策略”命令，出现“本地安全策略”窗口，如图 5-31 所示。

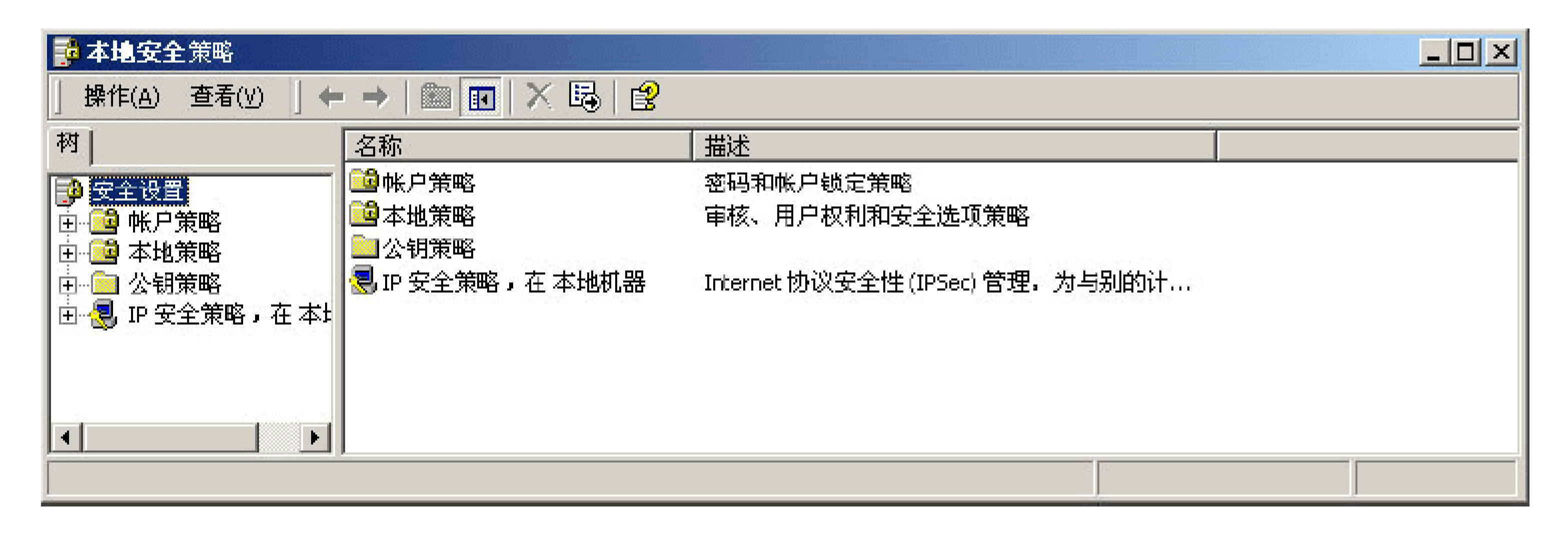


图 5-31　本地安全策略窗口

② 在本地安全策略窗口的左边选择“安全设置”|“本地策略”|“安全选项”，在右边窗口中找到“重命名系统管理员账户”并双击，出现“本地安全策略设置”对话框，如图 5-32 所示。

③ 在“本地安全策略设置”文本框中输入新的系统管理员账号名称，然后单击“确定”按钮，系统管理员账号名称就改变了。

修改系统管理员账号密码的具体操作如下。

① 选择“开始”|“程序”|“管理工具”|“计算机管理”命令，出现“计算机管理”窗口，如图 5-29 所示。

② 在“计算机管理”窗口左边中，依次选择“系统工具”|“本地用户和组”|“用户”，然后在右边窗口中右击 Administrator 项或者新设置的系统管理员账号，在出现的菜单中选择“设置密码”菜单项，出现“设置密码”对话框。如图 5-33 所示。

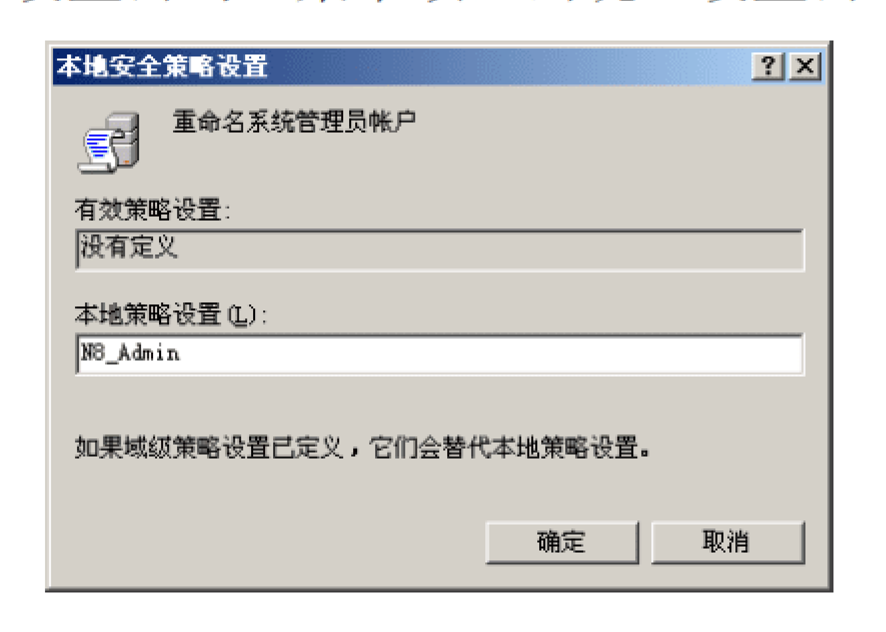


图 5-32 “本地安全策略设置”对话框



图 5-33 “设置密码”对话框

③ 在“新密码”文本框中输入密码，在“确认密码”文本框中再次输入同样的密码，单击“确定”按钮，系统管理员账号的密码就设置好了。

用户可以根据自己的习惯设置密码，为了密码设置有一定的安全性，可以通过本地安全策略来设置密码的规范。

具体的操作步骤如下。

① 选择“开始”|“程序”|“管理工具”|“本地安全策略”命令，出现“本地安全策略”窗口，如图 5-31 所示。

② 在本地安全策略窗口的左边选择“安全设置”|“账户策略”|“密码策略”，在右边窗口中找到“密码必须符合复杂性要求”并双击，出现“本地安全策略设置”对话框，如图 5-34 所示。

③ 选择“已启用”单选按钮，点击“确定”按钮，这里的设置可以生效。

④ 在右边窗口中找到“密码长度最小值”并双击，出现“本地安全策略设置”对话框，如图 5-35 所示。

⑤ 在“密码必须至少是”微调按钮中设置数字 8，然后单击“确定”按钮，使设置生效。

另外还有“密码最长存留期”、“密码最短存留期”、“强制密码历史”、“为域中所有用户使用可还原的加密来储存密码”也可以用同样的方法根据需要进行设置，一般情况下这几项使用默认设置就可以了。





图 5-34 “本地安全策略设置”对话框

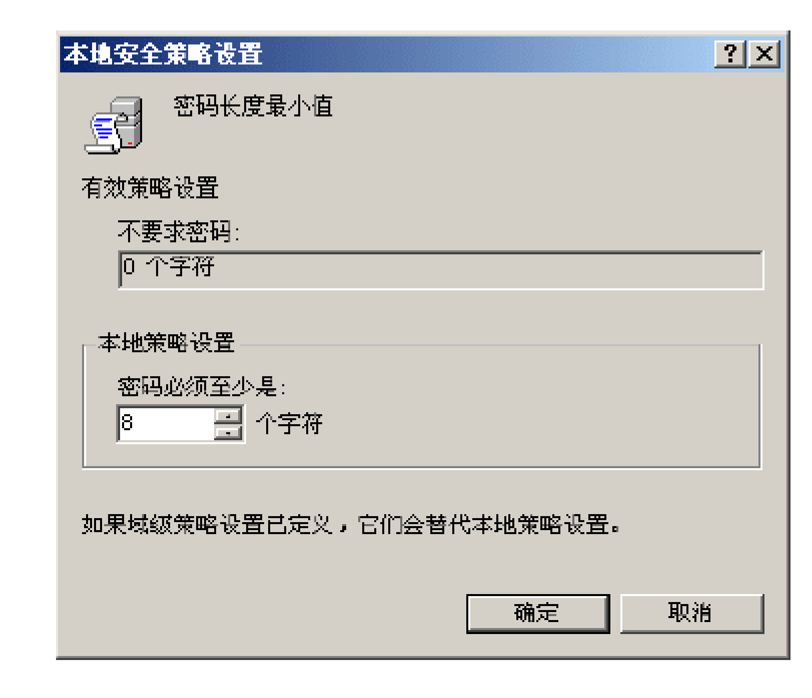


图 5-35 “本地安全策略设置”对话框

10. 本地策略

通过本地策略的合理配置，可以让系统记录相关的操作信息，以便在必要的时候可以检查计算机系统是否被别人操作过，或者受到过攻击。

具体的操作方法如下。

（1）选择“开始”|“程序”|“管理工具”|“本地安全策略”命令，出现“本地安全策略”窗口，如图 5-31 所示。

（2）在本地安全策略窗口的左边选择“安全设置”|“本地策略”|“审核策略”，在右边窗口中找到“审核策略更改”并双击，出现“本地安全策略设置”对话框，如图 5-36 所示。

（3）选择“成功”和“失败”两个复选框，表示会同时审计成功和失败事件，单击“确定”按钮，使设置生效。

（4）在右边窗口中找到“审核登录事件”并双击，出现“本地安全策略设置”对话框，如图 5-37 所示。

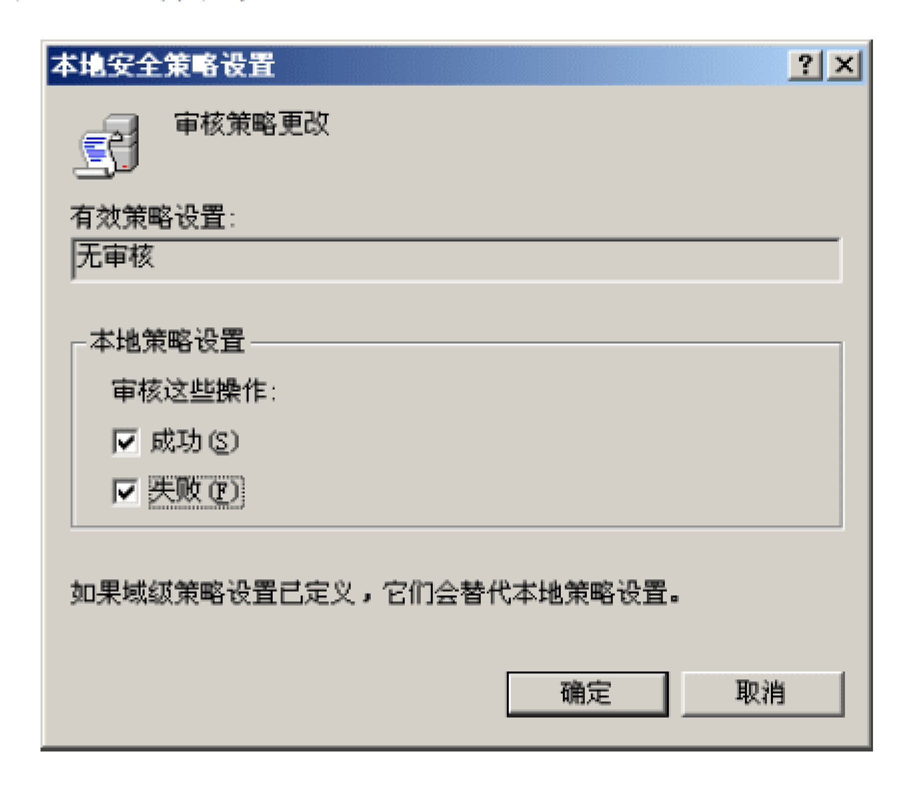


图 5-36 “本地安全策略设置”对话框

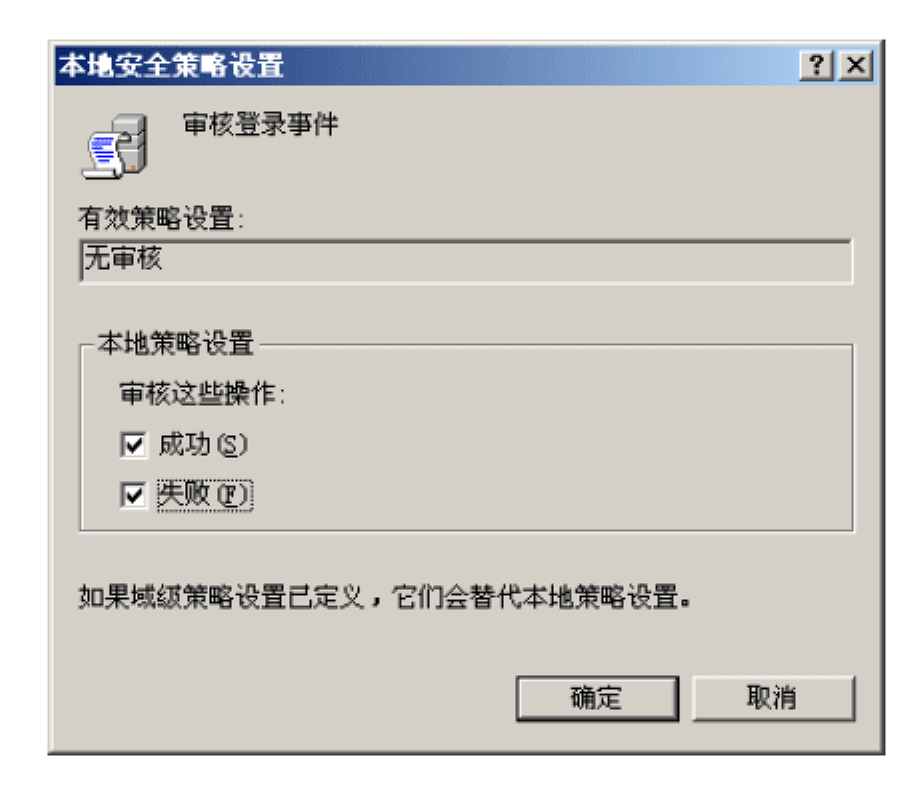


图 5-37 “本地安全策略设置”对话框

（5）选择“成功”和“失败”两个复选框，表示会同时审计成功和失败事件，单击“确定”按钮，使设置生效。

依照同样的方法对“审核对象访问”设置失败审核、“审核过程追踪”设置不审核、“审核目录服务访问”设置失败审核、“审核特权使用”设置失败审核、“审核系统事件”设置成功和失败审核、“审核账户登录事件”设置成功和失败审核、“审核账户管理”设置成功和失败审核。

设置审核以后，系统会产生日志信息，所以我们还需要设置事件日志文件的大小，以

满足系统记录日志信息的需要，具体步骤如下。

（1）选择“开始”|“程序”|“管理工具”|“事件查看器”命令，出现“事件查看器”窗口，如图 5-38 所示。

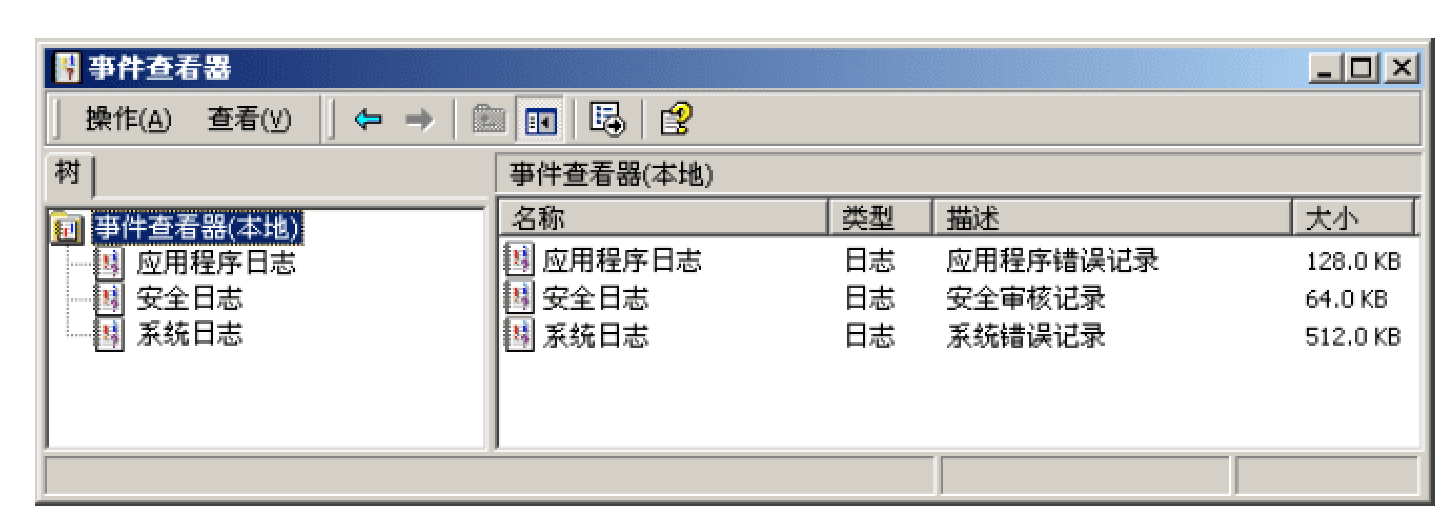


图 5-38　“事件查看器”窗口

（2）右键单击窗口左边的“应用程序日志”项，在弹出菜单中选择“属性”命令，出现“应用程序日志 属性”对话框，如图 5-39 所示。

（3）在“常规”选项卡下的“最大日志文件大小” 微调按钮中设置日志文件最大的容量为 51200KB，即 50MB，在“当达到最大的日志尺寸时”选择“不改写事件”单选按钮，单击“确定”按钮使设置生效。

（4）依照同样的方法可以将“安全日志”和“系统日志”的日志文件最大的容量也设置为 51200KB，并设置为“不改写事件”。

11. 查看本机打开的端口

有时为了确认计算机上是否有木马程序，需要查看计算机上开放了哪些端口，具体的操作方法如下。

选择“开始”|“运行”命令，在文本框中输入 CMD，出现命令行窗口，在命令行窗口中输入 netstat -a 并按回车键，如图 5-40 所示。

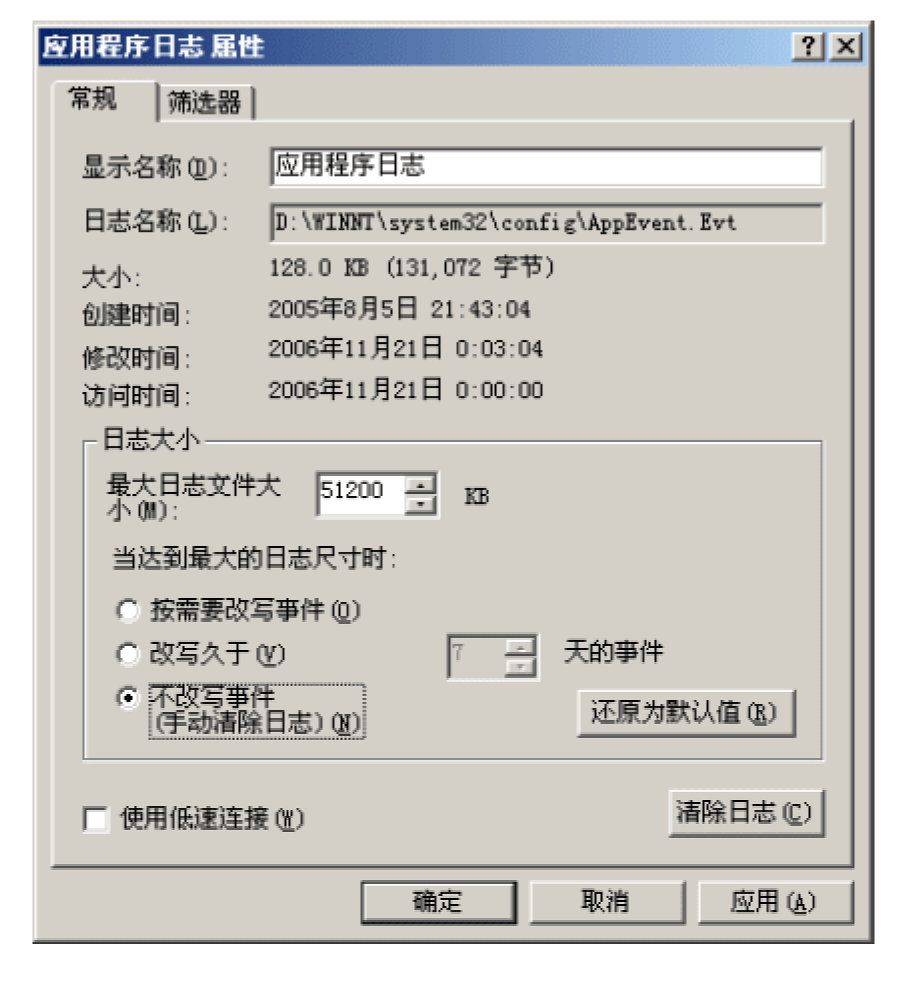


图 5-39　“应用程序日志属性”对话框

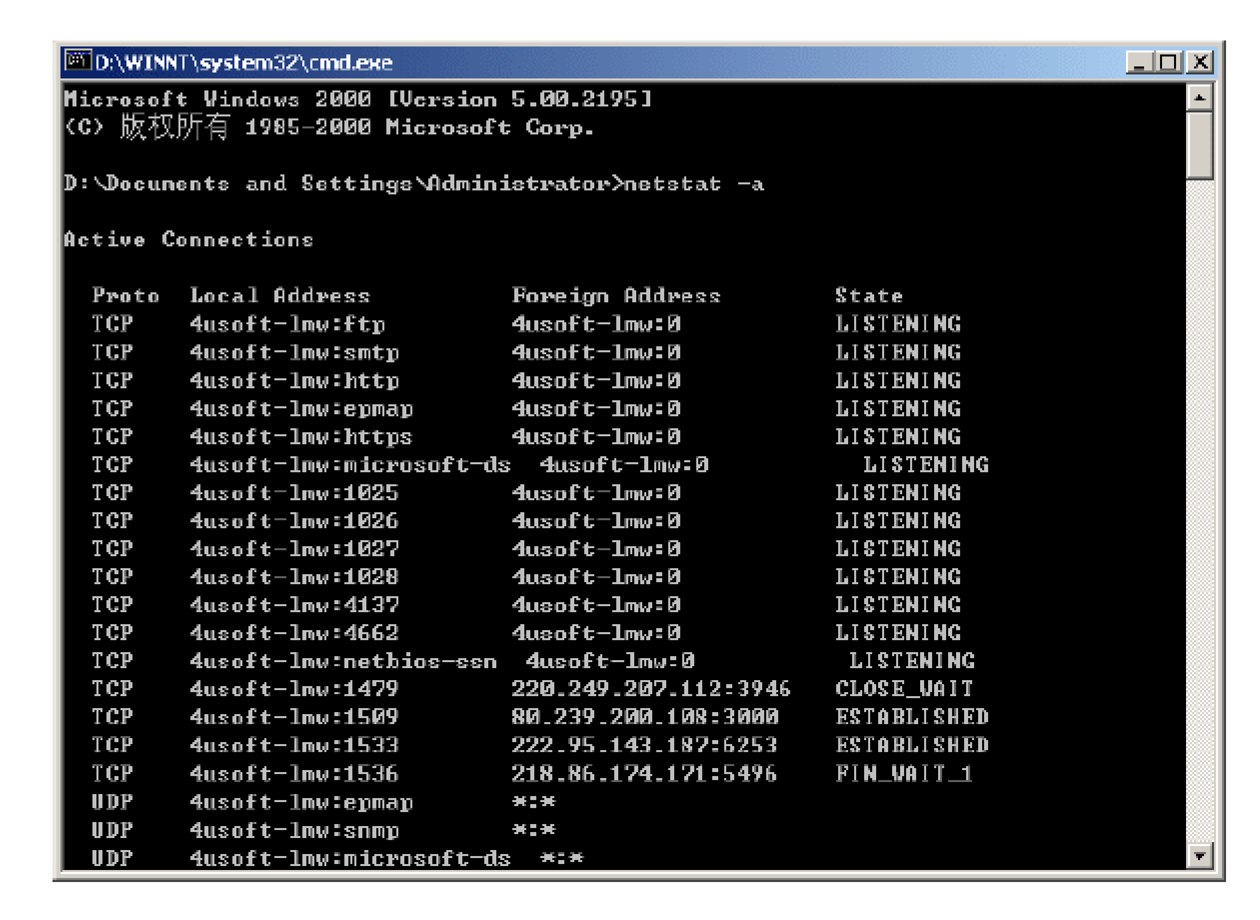


图 5-40　查看本机端口界面

5.1.3　系统备份

操作系统常常会因为各种各样的原因而崩溃，如硬件故障、软件损坏、病毒侵袭、黑客骚扰，或者是我们自己的误操作而造成的危险在时刻威胁着我们。系统崩溃或产生了重大错误以后，最好的办法就是重装系统。但是，为了保护原有操作系统中的相关配置和重

要数据不至于因为重新安装系统而丢失或者破坏，在重装之前，我们首先应该做的就是对系统中的重要信息进行备份，那么哪些是系统中的重要信息呢，下面我们将详细讲解。

1．备份硬盘数据

硬盘数据包括主引导扇区、操作系统引导扇区、FAT 表、DIR 表等，这是计算机系统赖以正常启动的基础，因此，及时备份好硬盘数据是首要的事情。对于硬盘数据的备份，最好的方法莫过于杀毒软件了，推荐使用“瑞星”杀毒软件，因为它不仅能够备份以上的硬盘数据，而且可以让用户设定自动备份的时间。

具体操作如下。

（1）选择“开始”|“程序”|“瑞星杀毒软件下载版”|“瑞星杀毒软件”命令，出现“瑞星杀毒软件下载版”窗口，如图 5-41 所示。

（2）选择“工具列表”选项卡，在列表中选择“硬盘数据备份”，单击右边的“运行”按钮，出现窗口如图 5-42 所示。



图 5-41　杀毒软件窗口



图 5-42　硬盘数据备份窗口

（3）单击“开始备份”按钮，开始进行硬盘数据备份，几分钟后硬盘数据就可以备份完成。

> **提示：**备份的硬盘数据只对当前硬盘分区状态有效，如果以后又对硬盘重新进行分区或调整了分区的大小，那么就应该重新备份。

2．备份注册表

注册表中存放着计算机的所有设置和各种软硬件的注册信息，所以它的重要性是不言自明的，因而及时备份注册表是一项极其重要的工作。

具体的操作步骤如下。

（1）选择“开始”|“运行”命令，在文本框中输入 regedit，出现“注册表编辑器”窗口，如图 5-17 所示。

（2）在“注册表编辑器”窗口中选择“注册表”|“导出注册表”命令，出现“导出注册表文件”对话框，如图 5-43 所示。

（3）在“保存在”下拉列表框中选择一个位置，再在“文件名”文本框中设置一个文件名，选择“全部”单选按钮，然后单击“保存”按钮，这样就完成注册表的备份了。

除了上述的备份方式以外，还可以直接将操作系统目录（如 C:\Windows）中的 User.dat

和 System.dat 两个文件复制出来，也能达到备份注册表的目的。

3．备份驱动程序

重装系统后，就需安装各种硬件的驱动程序，而查找、安装各类显卡、声卡的驱动时不但费时间，而且容易出现错误，实在是很麻烦的事情，如果丢失了驱动光盘，那更要费一番周折。这里介绍一种简单的方法来解决这个问题，在第一次安装完驱动程序以后，用“驱动程序备份专家”工具软件将驱动程序备份起来，下次重新安装以后，再恢复回去就好了。

具体的操作方法如下：

（1）选择“开始”|“程序”|“驱动程序备份工具”|“驱动程序备份工具”命令，出现驱动程序备份工具窗口，如图 5-44 所示。

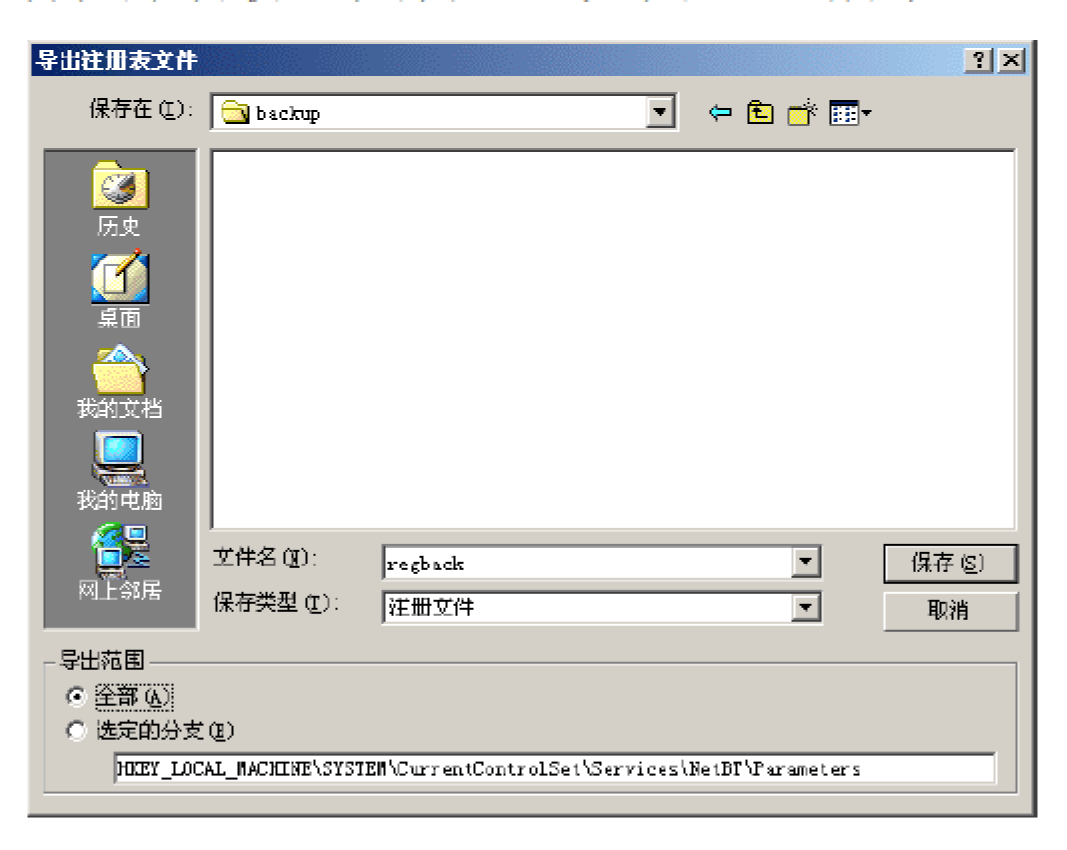


图 5-43 “导出注册表文件”对话框

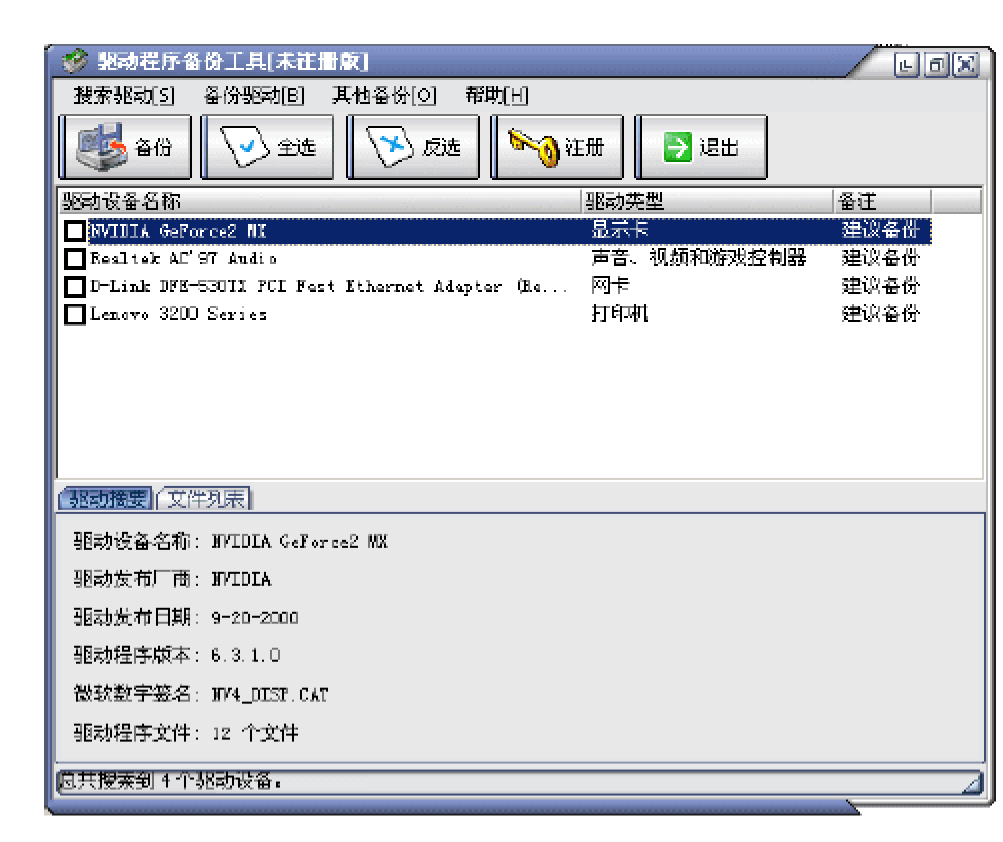


图 5-44 驱动程序备份专家窗口

（2）单击“全选”按钮，选择所有的驱动程序，然后单击“备份”按钮，出现“浏览文件夹”对话框，如图 5-45 所示。

（3）在“浏览文件夹”对话框中，选择一个保存备份的位置，单击“确定”按钮，这样就完成驱动备份了。

> **提示：**“驱动程序备份专家”工具软件可以从网上免费下载，然后安装到自己的计算机上。

4．备份邮件账号

当有多个 Outlook Express 邮件账号需要备份时，操作方法和注册表的备份基本上是一致的，所以这里只是简单说明一下，首先打开注册表编辑器，在注册表编辑器中依次展开到 HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts 分支，如果 Outlook Express 中有五个邮件账号，那么在 Accounts 键下就会有 00000001～00000005 五个子键。单击 Accounts 键，选择“注册表”|“导出注册表文件”命令，在“导出范围”中选择“选择的分支”，输入备份文件名，按“确定”按钮即可将它们备份出来。

5．备份个人资料

个人资料是计算机用户最重要的数据，包括个人文件、下载资料、个人邮件、OICQ 或 ICQ 数据等。

对于个人文件、下载资料的备份来说，我们只需将它们复制到硬盘的非系统分区或刻录到光盘等地方就行了。

对于个人邮件的备份来说，如果使用的是 Outlook Express，那么，就应该将 C:\Documents and Settings\User name\Local Settings\Application Data\Identities\{数字串}\Microsoft\Outlook Express\目录中的“收件箱.dbx”和“发件箱.dbx”两个文件复制到非系统区。当然，最好是平时就将邮件位置自定义到其他地方，具体的步骤是：

（1）选择“开始”|“程序”| Outlook Express 命令，出现 Outlook Express 窗口，如图 5-46 所示。

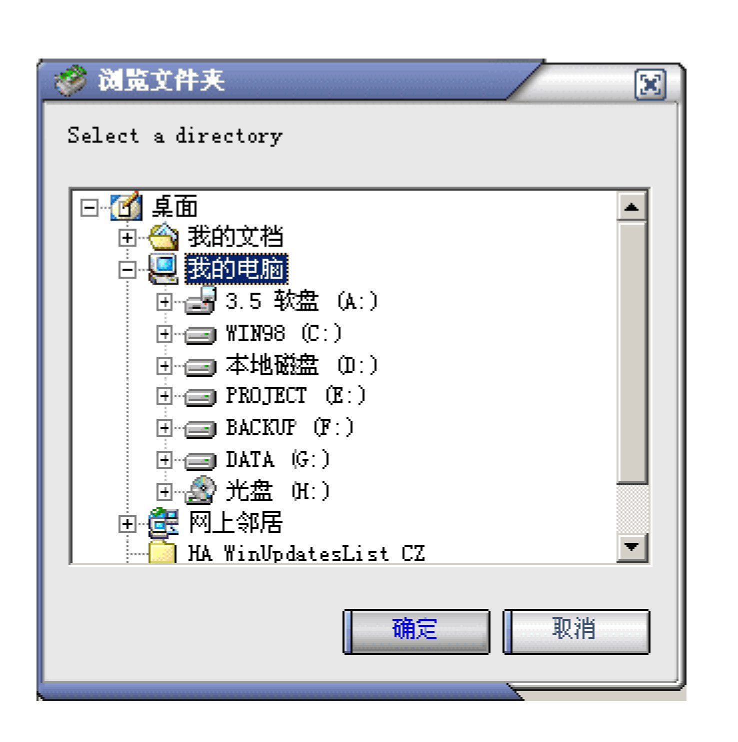


图 5-45　“浏览文件夹”对话框

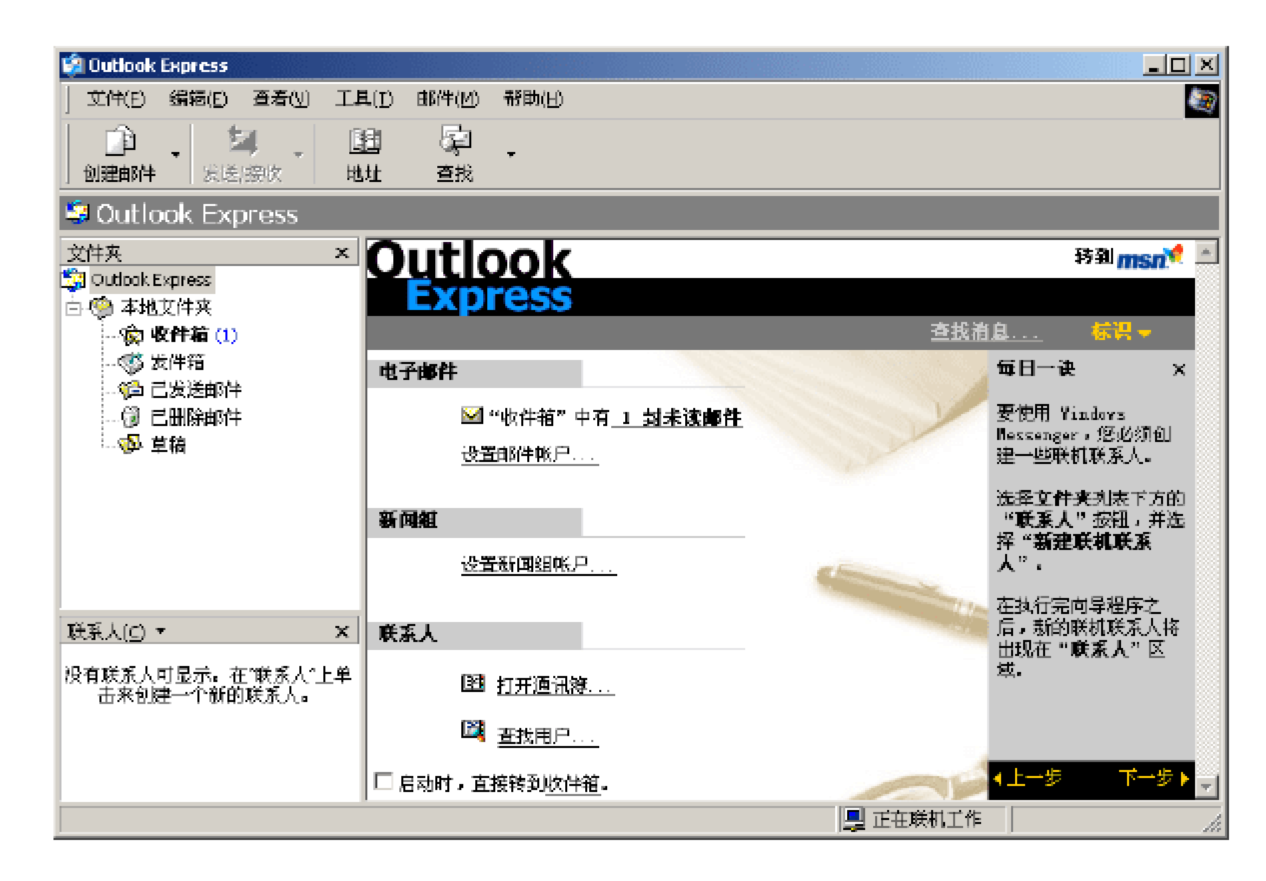


图 5-46　Outlook Express 窗口

（2）在 Outlook Express 窗口中，选择“工具”|“选项”命令，出现“选项”对话框，如图 5-47 所示。

（3）单击“存储文件夹”按钮，出现“存储位置”对话框，如图 5-48 所示。

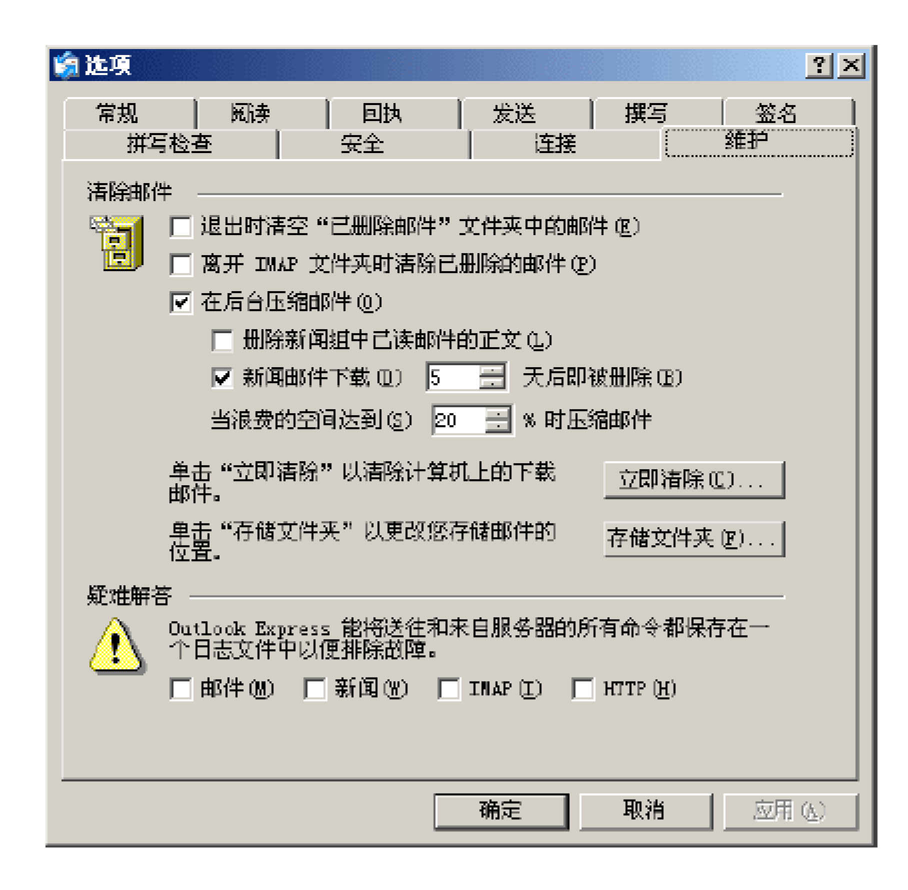


图 5-47　“选项”对话框



图 5-48　“存储位置”对话框

（4）单击“更改”按钮，出现“浏览文件夹”对话框，如图 5-49 所示。

（5）在“浏览文件夹”对话框中，选择希望保存的文件夹，然后单击“确定” 按钮，保存设置的位置。

这样就完成了 Outlook Express 默认邮件数据存储位置的修改了。

而对于备份 Foxmail 邮件来说则比较简单，只需将 Foxmail 安装目录下的 Mail 子目录中的文件复制到非系统区就行了。

OICQ 与 ICQ 的备份：对于 OICQ 来说，聊天记录和个人信息都存放在本地，最简单的方法就是把 OICQ 的安装文件夹中与自己 OICQ 号同名的子文件夹复制出来就行。当然，

也可以利用 OICQ 提供的“导出”功能也能备份聊天记录。ICQ 却与 OICQ 不同，ICQ 并没有将好友名单保存在服务器中，而是保存在了客户端，因此，在重装系统后，不仅要重复输入自己的 ICQ 号和密码，而且还要重新输入好友们的 ICQ 号进行搜索并等待他们的确认，操作过程极为繁琐。所以，我们应该利用第三方软件来完成备份工作，在这里，向大家推荐使用 ICQ Rescue 这款专门备份 ICQ 的免费软件，使用非常简单，并且有详细的提示，具体的操作就不多说了。

6. 备份通信簿

对于通信簿的备份，只需将“系统盘\Documents and Settings\用户名\Application Data\Microsoft\Address Book”中的文件复制到非系统区即可。

当然，我们也可通过邮件软件本身来备份，具体操作如下。

（1）选择“开始”|“程序”| Outlook Express 命令，出现 Outlook Express 窗口，如图 5-46 所示。

（2）选择“文件”|“导出”|“通信簿”命令，出现“通信簿导出工具”对话框，如图 5-50 所示。



图 5-49 “浏览文件夹”对话框

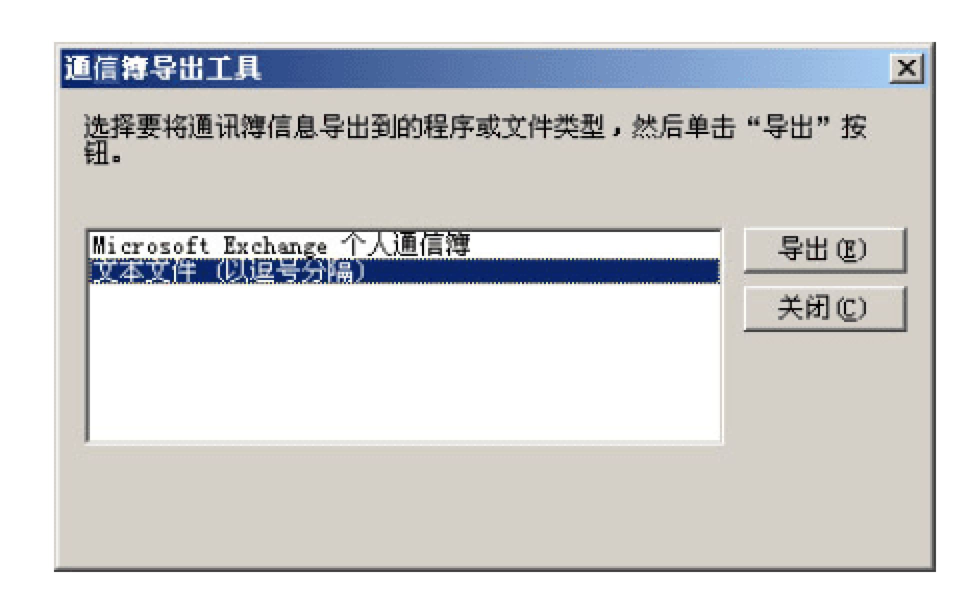


图 5-50 “通信簿导出工具”对话框

（3）选择一种格式，一般选择“文本文件（以逗号分隔）”，然后单击“导出”按钮，出现“CVS 导出”对话框，如图 5-51 所示。

（4）在“将导出文件另存为”文本框中输入文件位置和文件名，然后单击“下一步”按钮，此时可以选择要导出的内容，如图 5-52 所示。



图 5-51 “CSV 导出”对话框



图 5-52 “选择导出的内容”对话框

（5）单击希望导出的项目，使其处于选中状态，设置完成后，单击“完成”按钮，此时完成通信簿备份。

7．备份邮件规则与个性化签名

通过定制邮件规则可以有效地防止垃圾邮件，这些规则可以在脱机状态下设定，因此，邮件规则的备份也是一项很重要的工作。邮件规则的备份可以借助于注册表编辑器，找到 HKEY_CURRNT_USER\Identities\{77BEB813-E85F-411A-9704-CA8F14492CC2}\Software\Microsoft\Outlook Express\5.0\Rules\Mail，该主键中保存着邮件规则设置，当然，用户不同，那么大括号中的数据也会有所不同，将 Mail 主键导出，即可完成邮件规则的备份。

个性化签名可以有两种不同的实现方式，一是文本方式，即直接在 Outlook Express 中输入；二是文件方式，即指定某文件作为签名，并附加在邮件的末尾。对于后者，备份自然非常简单。而备份前者就需要在注册表中进行操作。个性化签名位于注册表中 HKEY_CURRNT_USER\Identities\{77BEB813-E85F-411A-9704-CA8F14492CC2}\Software\Microsoft\Outlook Express\5.0 主键下的 Signatures 键值项中，导出 Signatures 也就备份了个性化签名。

8．备份 IE 收藏夹

IE 收藏夹中的 BOOKMARKS 存放在 X:\Documents and Settings\用户名\Favorites\目录中的许多 URL 链接，把它们复制出来即可完成备份工作，而当重新安装好系统后再将其复制到原来的目录下即可完成恢复。除此以外，我们还可以利用 IE 的“导出”功能、改变收藏夹存放路径来实现备份。

（1）利用 IE 的“导出”功能，具体操作如下。

① 选择“开始”|“程序”| Internet Explore 命令，出现 Internet Explore 窗口，如图 5-53 所示。

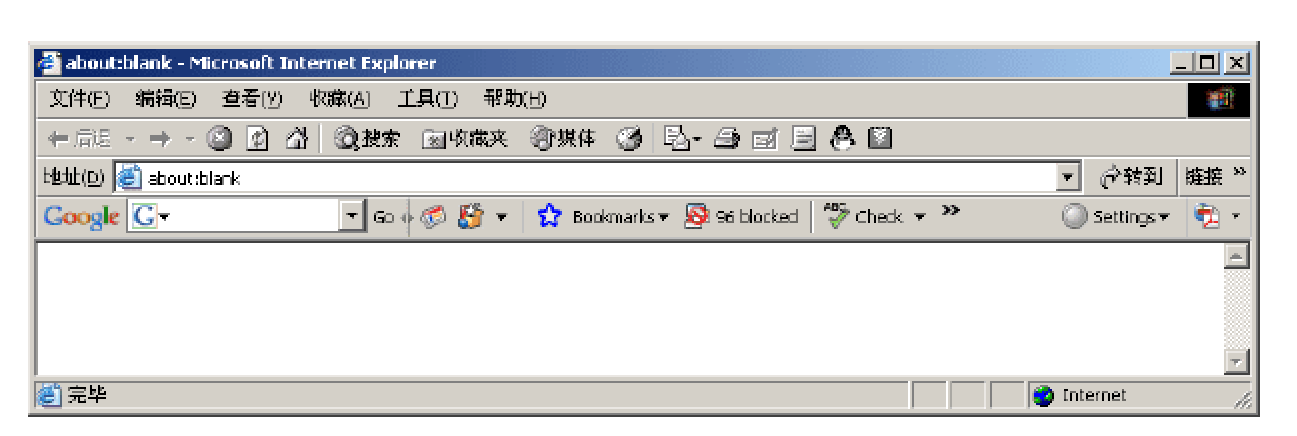


图 5-53　Internet Explore 窗口

② 选择“文件”|“导入和导出”，出现“导入/导出向导”对话框，如图 5-54 所示。

③ 单击“下一步”按钮，可以选择需要进行的操作，这里选择“导出收藏夹”，如图 5-55 所示。



图 5-54　导入/导出向导

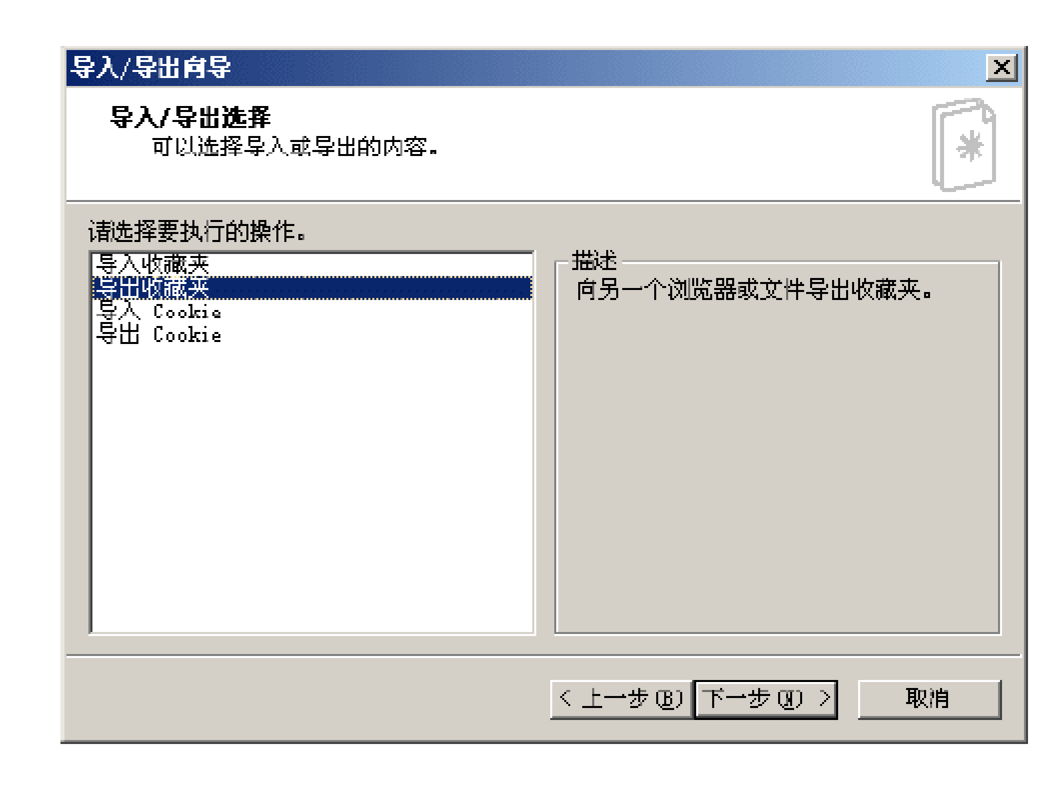


图 5-55　选择要执行的操作

④ 单击“下一步”按钮，提示需要从哪个文件夹开始导出，如图 5-56 所示。

⑤ 选择好要导出的文件夹以后，单击“下一步”按钮，提示输入导出文件的路径和文件名，如图 5-57 所示。

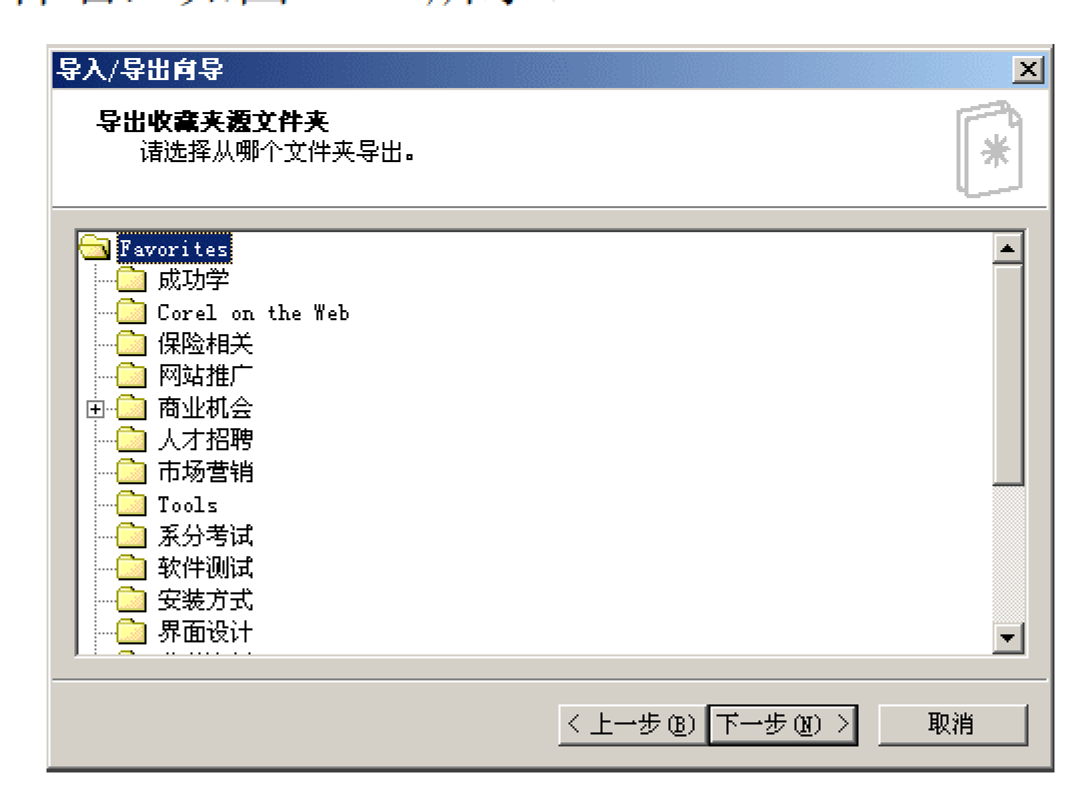


图 5-56 选择导出文件夹



图 5-57 设置导出文件路径和名称

⑥ 设置好导出文件的路径和名称以后，单击“下一步”按钮，导出程序自动完成。

（2）改变收藏夹存放路径，具体操作如下：

在注册表编辑器中展开到 HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Explorer\Shell Folders 分支，在右窗口中找到 Favorites 键值项，双击它后，在“数据数值”中输入 E:\favorites 即可。这样，以后收藏夹中的内容都存放到了 E 区中（如果 E 区是非系统区）。

9. 备份自定义词组

平时，我们为了更方便、快捷地输入词组，经常会自己定义一些词组，但系统一旦崩溃，这些自定义的词组也就会随之“牺牲”，那么，我们就应该将它们加以备份，以供重装系统后再用。在 C:\Windows\System32\文件夹中，Wbx.emb、tmmr.rem、pXXXp.upt 三个文件分别对应着五笔输入、智能拼音、微软拼音三种输入法的自定义词组（其中的 XXX 是登录系统时输入的用户名），把它们复制出来就行了。另外，对于手工造词，可以利用它的“功能菜单”中的“自造词工具”自带的“导出”命令将其保存到其他位置，这样的保存也能达到备份的目的。

10. 备份系统分区

备份系统分区，一个方法是用 Ghost 备份整个系统盘，另外一个方法是使用 Windows XP 自带的“系统还原”功能来备份。

（1）使用 Ghost 备份的方法如下：

① 启动 Ghost 备份程序，界面如图 5-58 所示。

② 选择 Local | Partition | To Image 命令，弹出选择硬盘窗口，如图 5-59 所示。

③ 从列表中选择硬盘，然后单击 OK 按钮，出现选择分区的窗口，如图 5-60 所示。

④ 用鼠标单击列表项选择要备份的分区，完成后，单击 OK 按钮，要求设置备份文件存放路径和文件名，如图 5-61 所示。

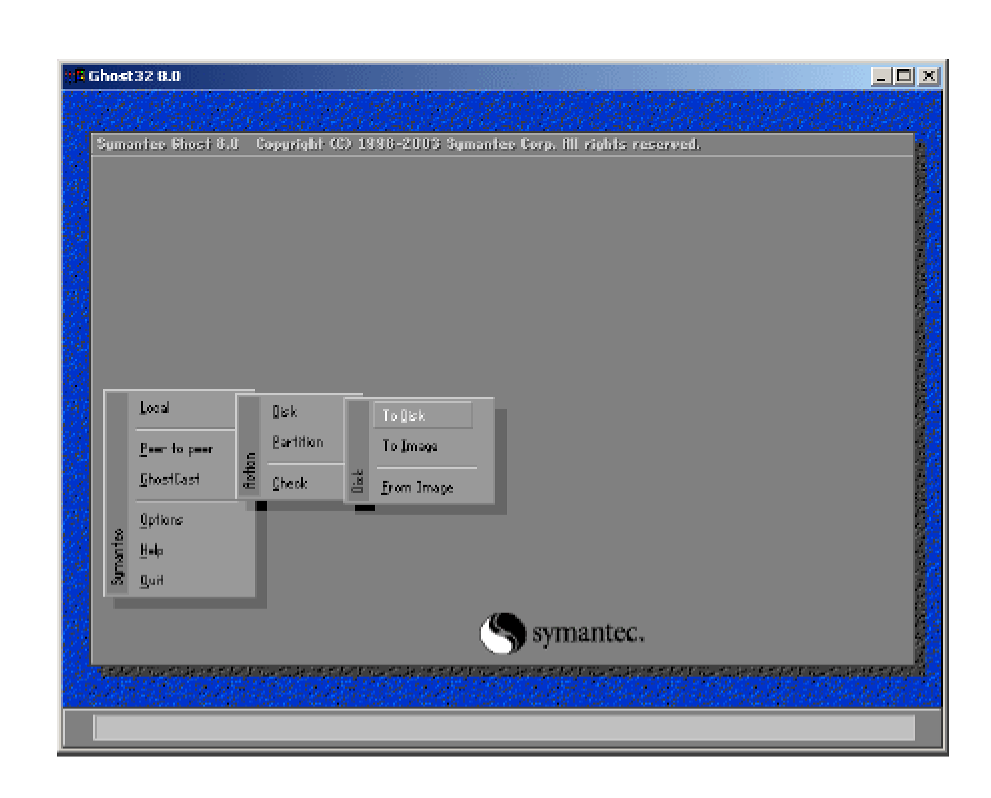


图 5-58　Ghost 备份程序

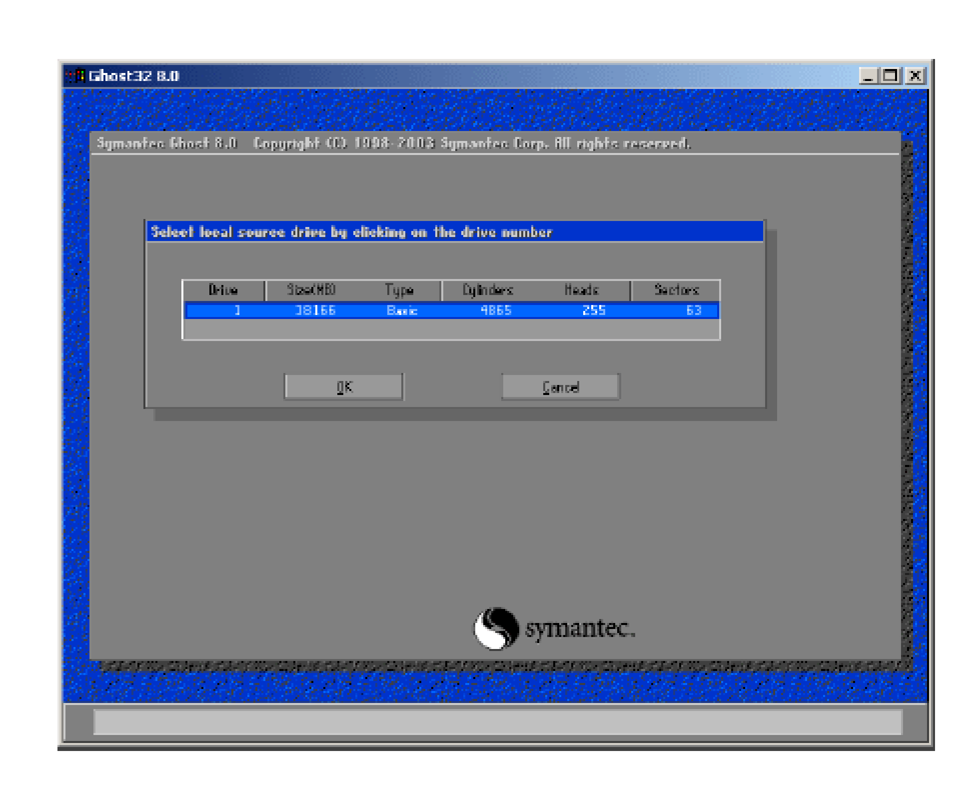


图 5-59　选择硬盘

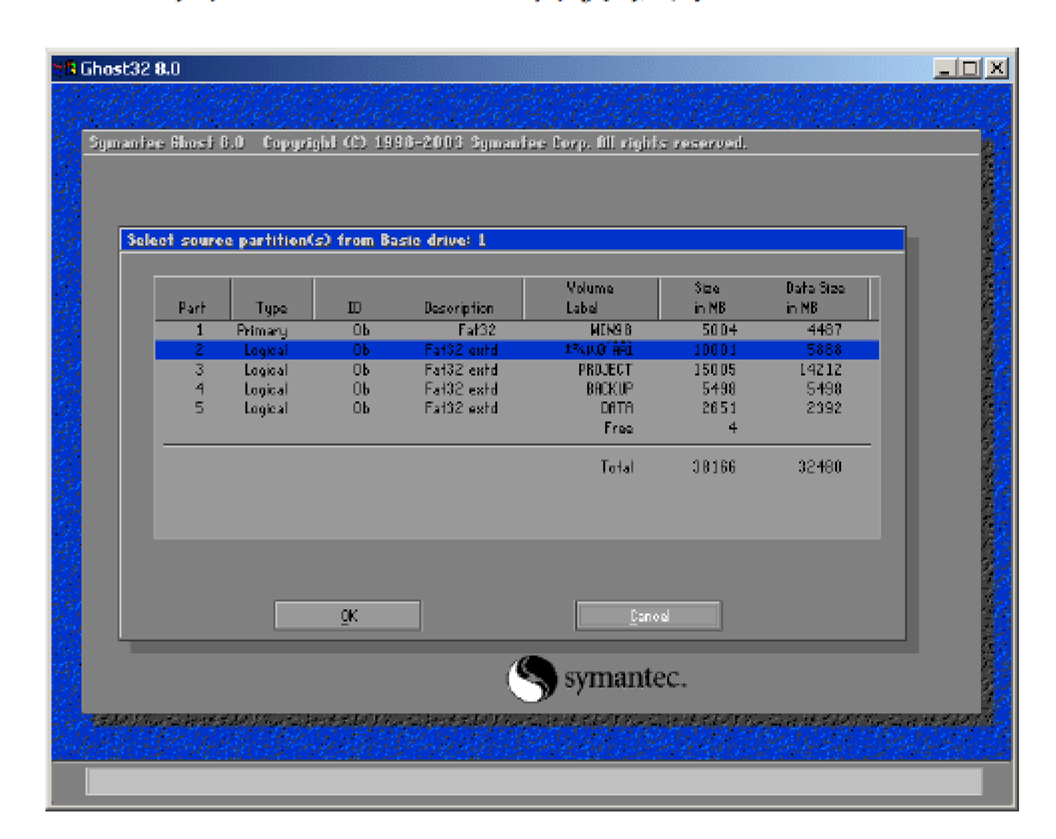


图 5-60　选择要备份的分区

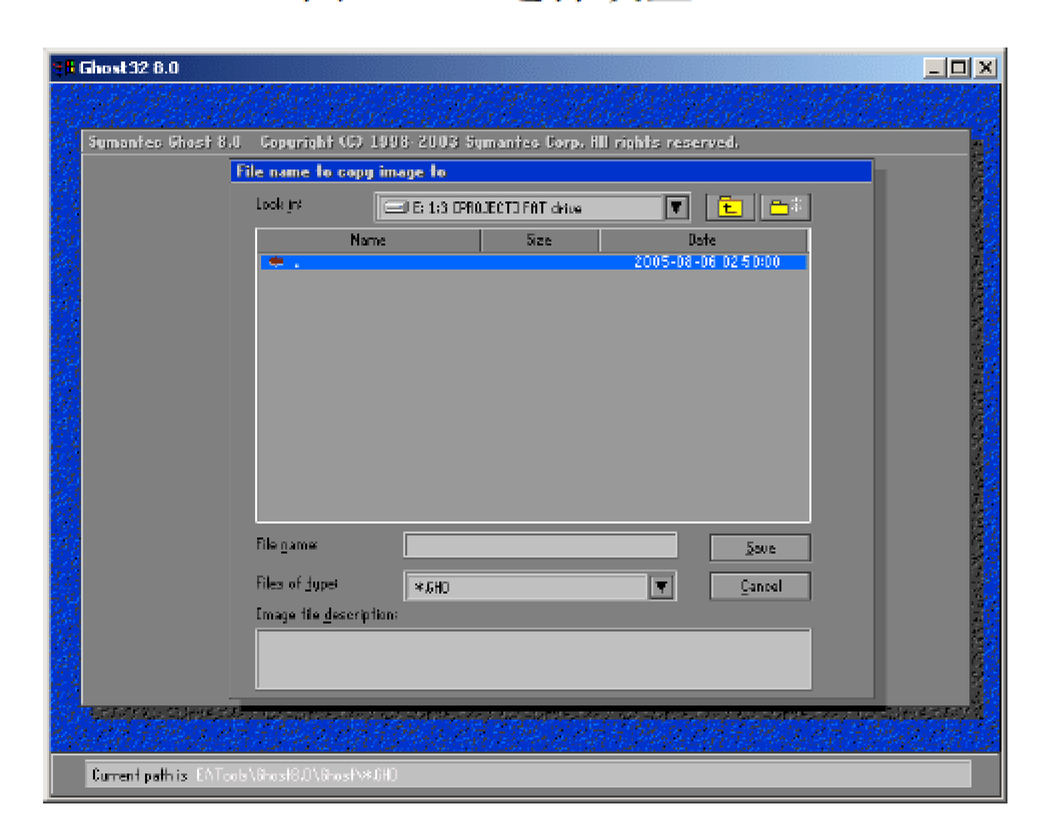


图 5-61　设置备份文件路径和文件名

⑤ 设置完成备份路径和文件名后，单击 Save 按钮，备份程序开始备份，备份完成时系统会提示，备份完成。

（2）使用 Windows XP 自带的“系统还原”功能来备份，操作比较简单，希望读者自己作为练习来完成这种方式的备份。

认真做好备份工作，当系统崩溃时才不至于后悔莫及。

5.1.4　反间谍软件

间谍软件是一种通用术语，用于描述执行某些特定任务的软件，例如，在未经您同意或控制的情况下，收集个人信息或更改您计算机的配置。 间谍软件可使您的计算机速度明显变慢，对关键设置进行更改，并且难以删除它们。

反间谍软件可以通过检测和删除已知间谍程序来帮助保护您的计算机免受间谍软件和其他潜在不受欢迎的软件的攻击。您可以安排该软件在您方便时对您的计算机进行扫描。

1．什么是间谍软件

间谍软件是执行某些行为（例如广告、收集个人信息或通常没有经过您的同意就更改计算机的设置）的软件的通用术语。 如果出现以下情况，您的计算机上就可能存在间谍软件或其他有害的软件。

（1）甚至您不在 Web 上也会看见弹出式广告。

（2）您的 Web 浏览器首先打开的页面（主页）或您的浏览器搜索设置已在您不知情的情况下被更改。

（3）您注意到浏览器中有一个您不需要的新工具栏，并且发现很难将其删除。

（4）您的计算机完成某些任务所需的时间比以往要长。

（5）计算机崩溃的次数突然上升。

间谍软件通常和显示广告的软件（称为“广告软件”）或跟踪个人或敏感信息的软件联系在一起。这并不意味着所有提供广告或跟踪您的在线活动的软件都是恶意软件。例如，您可能要注册免费音乐服务，但代价是要同意接收目标广告。 如果您理解并同意该条款，您可能已确定这是一桩公平交易。 您也可能同意让该公司跟踪您的在线活动以确定要显示的广告。

其他的有害软件会对您的计算机作出一些令人烦恼的更改，而且可能会导致计算机变慢或崩溃。这些程序能够更改 Web 浏览器的主页或搜索页，或者在您的浏览器中添加您不需要的附加组件。这些程序还会使您很难将您的设置恢复为原始设置。 这些类型的有害程序通常也称为间谍软件。

一切的关键在于您（或其他使用您的计算机的人）是否了解软件要执行的操作以及是否已同意将软件安装在您的计算机上。

间谍软件或其他有害的软件有多种方法可以侵入您的系统。常见的伎俩是在您安装需要的其他软件（如音乐或视频文件共享程序）期间偷偷地安装该软件。每当在计算机上安装程序时，请确保您已仔细阅读所有的公告，包括许可协议和隐私声明。有时在特定软件安装中已经记录了包括有害软件的信息，但是此信息可能出现在许可协议或隐私声明的结尾。

2．间谍软件的征兆

如果您的计算机开始有异常的表现或显示出下面所列的任何症状，则您的计算机上可能安装了间谍软件和其他有害的软件。

（1）我老是看见弹出式广告。一些有害的软件会连珠炮似的弹出与当前访问的特定 Web 站点无关的广告。这些广告通常是令人反感的其他 Web 站点。如果您在刚打开计算机时，甚至还没开始浏览 Web 时就看见弹出式广告，您的计算机上就可能存在间谍软件或其他有害的软件。

（2）我的设置已被更改，但是我不能将其恢复原状。一些有害的软件能够更改您的主页或搜索页设置。这意味着您启动 Internet 浏览器时首先打开的页面或您选择“搜索”时出现的页面可能是您不认识的页面。即使您知道如何调整这些设置，您可能会发现在您每次重新启动计算机时，这些设置又会恢复原状。

（3）我的 Web 浏览器含有我印象中没有下载过的附加组件。 间谍软件和其他有害的软件会将您不需要的附加工具栏添加至 Web 浏览器。即使您知道如何删除这些工具栏，在您重新启动计算机时它们也会恢复原状。

（4）我的计算机的速度似乎很慢。间谍软件和其他有害的软件不一定是高效的软件。这些程序会使用资源跟踪您的活动和弹出广告，从而降低计算机运行速度，而且软件的错误可能会使计算机崩溃。 如果您发现某种程序崩溃的次数突然增加，或者如果您的计算机在执行常规任务时慢于正常速度，您的机器上就可能存在间谍软件或其他有害的软件。

3．如何除去间谍软件

各种各样有害的软件（如间谍软件）都被设计成很难删除。 如果您尝试像卸载任何其

他程序一样卸载这种软件，您可能会发现在重新启动计算机后这种程序会马上重新出现。如果您在卸载有害的软件方面有困难，您可能需要下载一个工具帮助您卸载。几个公司提供免费且低成本的软件，这些软件会在您的计算机上检查间谍软件和其他有害的软件并帮助您删除它们。

一些 Internet 服务提供商 (ISP) 在其服务包里包含有防间谍软件的软件。与您的 ISP 协商，看他们是否可以建议或提供工具。如果您的 ISP 没有提供间谍软件和其他有害软件的删除工具，您可以请求您信任的人建立一个工具或参见下面列出的几个著名的工具。切记使用这些工具删除有害的软件可能意味着您不再能够使用其携带的免费程序。

要删除间谍软件，请执行以下操作。

（1）下载新的Microsoft Windows AntiSpyware 或者其他的间谍软件删除工具。

（2）运行该工具扫描计算机以查找间谍软件和其他有害的软件。

（3）在该工具发现的所有文件中检查间谍软件和其他有害的软件。

（4）按照该工具的说明选择要删除的可疑文件。

4．如何防止间谍软件

间谍软件和其他有害的软件会侵犯您的隐私、连珠炮似的弹出窗口、使计算机变慢甚至崩溃。以下是几种帮助您防止计算机受间谍软件及其他有害软件侵入的方法。

（1）更新软件

如果您使用 Windows XP，您可以通过确保所有软件都已更新来帮助防止间谍软件和其他有害软件的侵入。首先，访问 Microsoft Update 确认“自动更新”已打开，并且已经下载了所有最新的关键性安全更新。

（2）调整您的 Internet Explorer Web 浏览器的安全设置。

您可以调整 Web 浏览器的安全设置，以便确定您愿意从 Web 站点接受的信息量。

如果您运行 Windows XP SP2 并且使用 Internet Explorer 浏览 Web，您的浏览器已经设置为防止间谍软件和各种各样的欺骗性或有害的软件。

要查看当前的 Internet Explorer 安全设置，请执行以下操作：

在 Internet Explorer 中，单击“工具”按钮，然后单击 Internet 选项，选择“安全”选项卡。

（3）使用防火墙

尽管大多数间谍软件、有害的软件和其他程序捆绑在一起或来自不择手段的 Web 站点，但是实际上有一小部分可能是黑客远程发送到您的计算机上的间谍软件。安装防火墙或使用 Windows XP 内置的防火墙可有效防范黑客。

（4）更安全地上网和下载

抵御间谍软件和其他有害软件的最好办法是先不要下载它。以下几个提示可以帮助您免于下载不需要的软件：

- 仅从您信任的 Web 站点下载程序。
- 阅读与下载的软件有关的所有安全警告、许可协议和隐私声明。
- 切勿通过单击“同意”或“确定”按钮来关闭窗口。总是使用右上角红色的“╳”。
- 谨防流行的“免费”音乐和电影文件共享程序，确信自己更清楚地了解这些程序所包含的所有软件。

（5）在计算机上安装防止间谍软件的应用程序，时常监察及清除电脑的间谍软件，以阻止软件对外进行未经许可的通信。

5．反间谍软件举例

反间谍软件是防止间谍软件的最简单、最有效的方式，在此以微软的反间谍软件 GIANT AntiSpyware 为例，说明如何使用反间谍软件。

（1）选择“开始”|“程序”| GIANT AntiSpyware | GIANT AntiSpyware 命令，出现 GIANT AntiSpyware 窗口，如图 5-62 所示。



图 5-62 反间谍软件主界面

（2）单击窗口右边的 Spyware Scan 按钮，进入扫描间谍软件窗口，如图 5-63 所示。

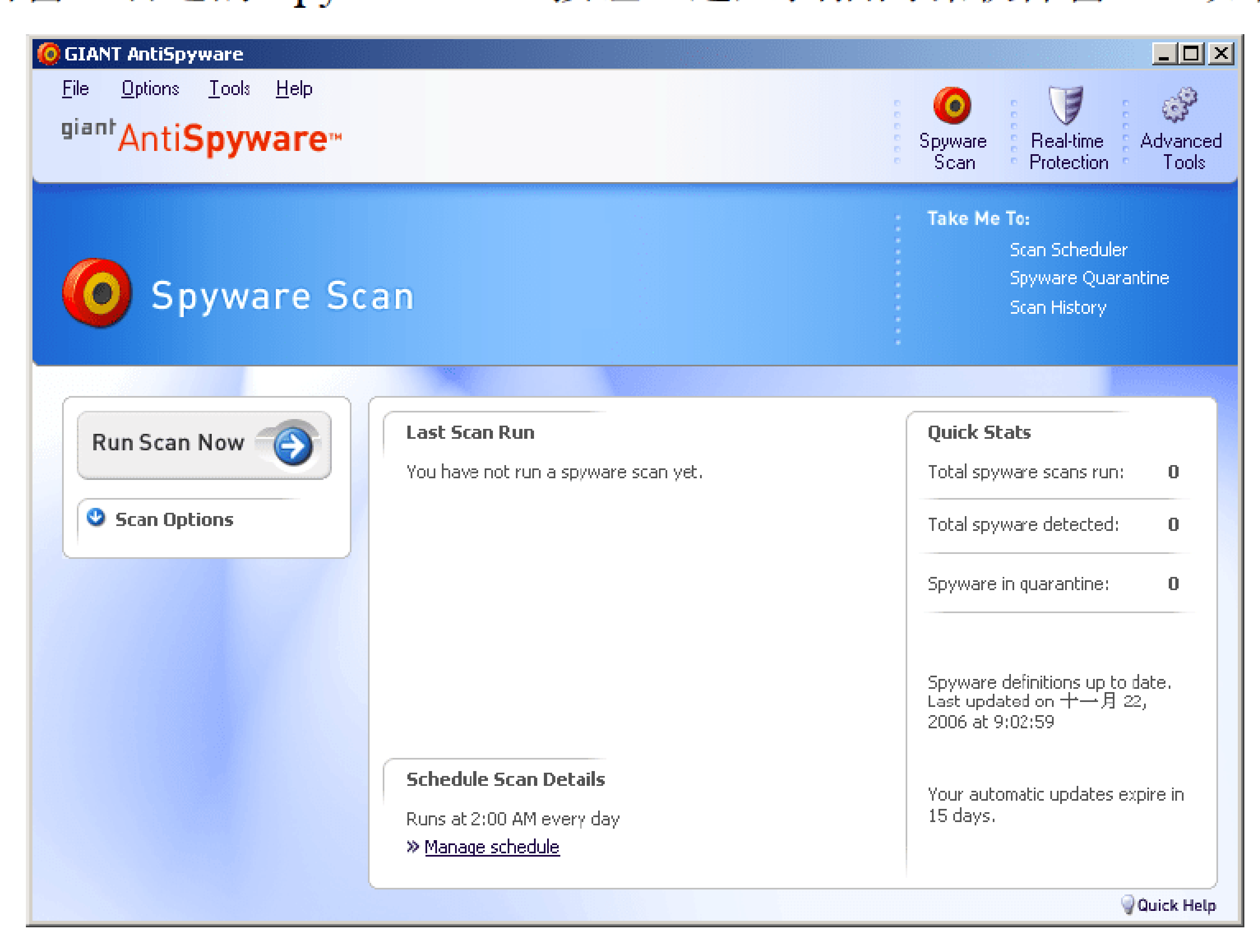


图 5-63 扫描间谍软件窗口

（3）单击窗口左边的 Run Scan Now 按钮，软件开始扫描系统中是否存在间谍软件，发现可疑程序会自动列在窗口中，如图 5-64 所示。

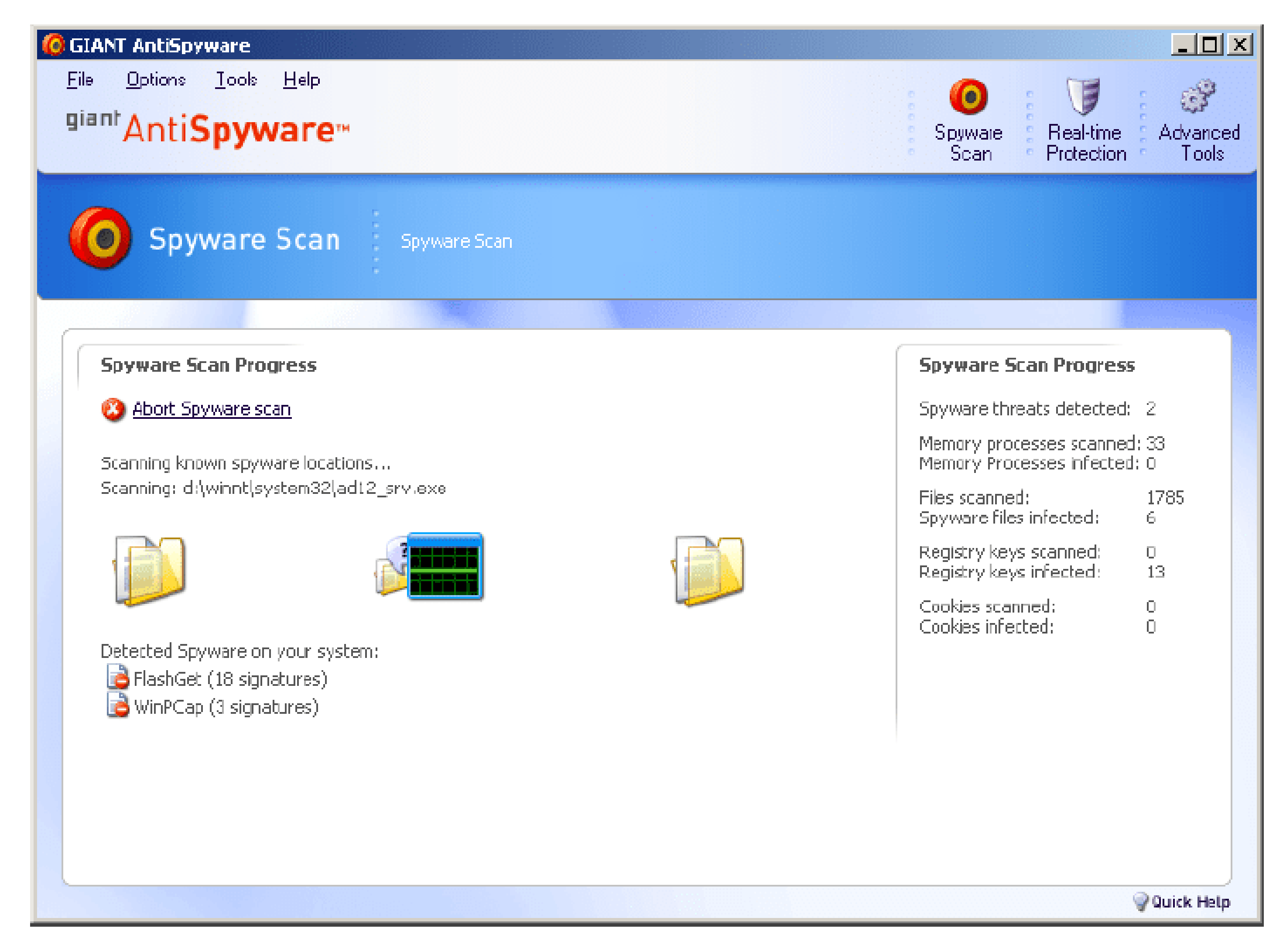


图 5-64 正在扫描间谍软件

（4）扫描完成的时候，出现一个扫描结果概要信息的窗口，如图 5-65 所示。

（5）单击 View Results 按钮，查看扫描结果信息，如图 5-66 所示。

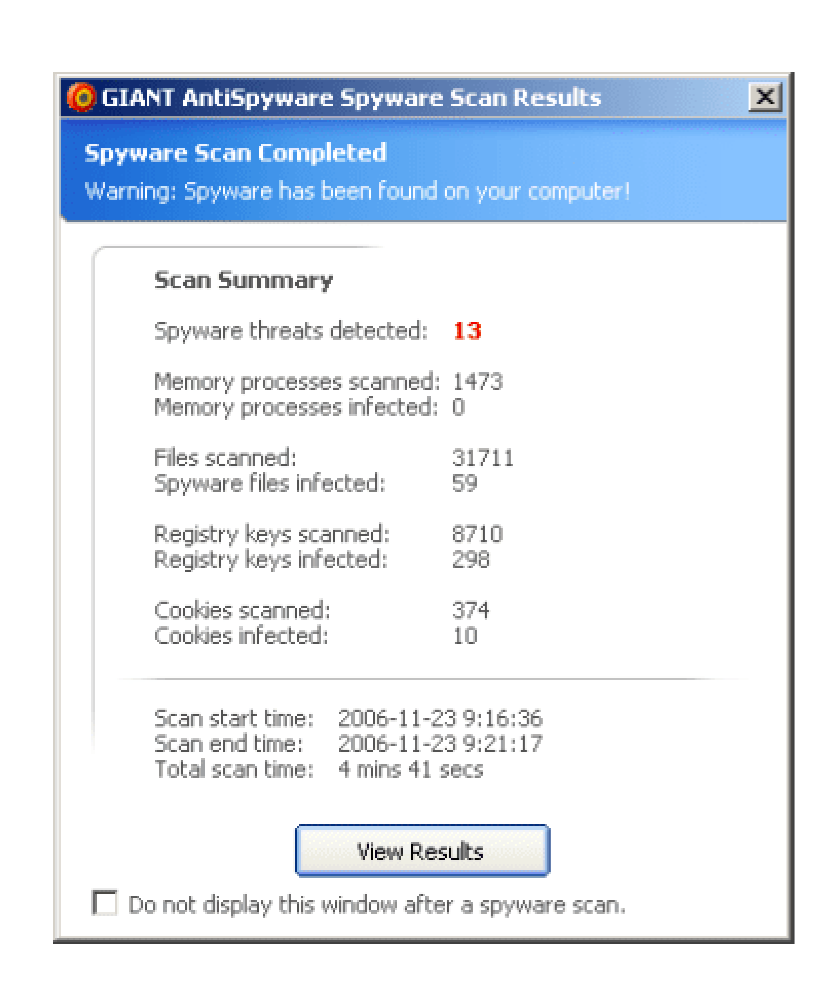




图 5-65 扫描结果概要信息窗口　　　　　图 5-66 扫描结果信息窗口

（6）窗口左边列表显示了扫描过程中发现的可疑程序，通过改变列表项前面的下拉列表框中的设置，可以对该程序设置为删除、隔离、忽略以及总是忽略。设置完成后，单击 Continue 按钮，出现提示是否确定要使配置生效，如图 5-67 所示。

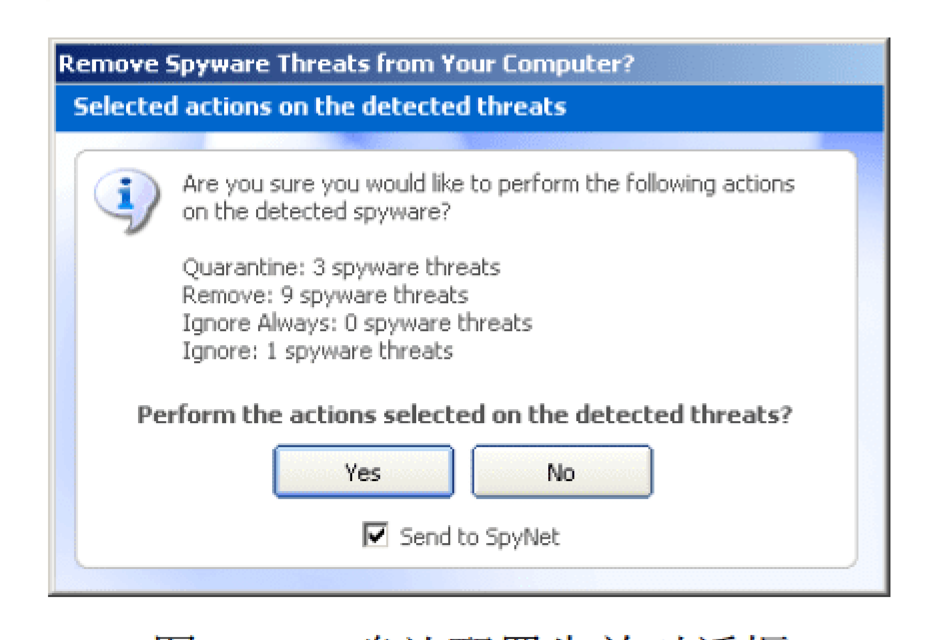


图 5-67 确认配置生效对话框

（7）单击 Yes 按钮，程序将按照刚才的配置对扫描到的间谍软件进行处理，这样一次完整的间谍软件扫描处理过程就完成了。

5.2 数据安全

前面我们对硬件安全、软件安全进行了探讨，这里我们针对计算机数据安全的相关内容进行探讨。数据可以说是我们最关心的内容，比如我们做的财务报表、项目规划、产品说明、市场报告等。

5.2.1 文件管理

计算机上几乎所有的信息都是以文件的形式来存储和管理的，所以确保计算机上文件的安全管理具有至关重要的意义。总的来说，文件分为两种，一种是系统文件；一种是数据文件。这里我们主要关心的是数据文件，因为其中包含着我们所关心的数据信息。

1. 家庭中的文件管理

在多数家庭中计算机存在的情况，一种情况是家庭成员共同使用，另一种情况是家里来的朋友也可能使用我们的计算机。

（1）误删除或误移动文件

有时我们会发现自己存储在某个位置的文件找不到了，也不知道是什么时候丢失的，这时候我们很可能去问家庭中使用过该计算机的每个人，是否删除了自己的文件，如果只是另外的一两个人用过还好，如果有多个人使用过，而且有些朋友也使用过，使用完了就离开了，我们这时也不好意思再去找朋友来问了。可是自己的文件丢失又特别着急，这可真是有苦难言啊。

出现上述情况的主要原因是使用计算机的操作人员对计算机的熟悉程度差别可能比较大，从而导致容易误操作，比如一不小心将一个文件或者文件夹拖到别的文件中，自己可能还没有注意到，也可能注意到了，但不知道怎样还原，也有可能是一不小心删除了，对不熟悉计算机操作的人员，除非是故意删除的，否则多数情况下是删除到回收站的。解决的方法是将计算机设置多个用户，不同的人使用时使用不同的用户名登录，同时对计算机上的文件操作情况进行监视，记录操作用户名、操作时间、操作类型、操作程序、操作原始文件、操作目标文件等信息，当出现问题的时候，只需要在记录的日志信息中就可以很容易查询到对具体文件的变动信息，再也不用一个一个去问使用过计算机的人。

（2）隐私信息被别人查看

每个人总是有一些自己的私人信息是不希望别人看到的。当然还有些信息是容许一些人看，而不方便另外一些人看的，比如自己家里的财务情况，爱人可以看，但是朋友就不方便了。对这些敏感信息的有效管理也是很有必要的。

针对这种情况，我们需要做的就是将敏感信息文件保护起来，比如隐藏起来，让其他的人员使用计算机时看不到我们的私人文件，同时禁止其他人对我们的文件进行查看、修改、删除、改名等操作，这样既保护我们的隐私信息，也保护我们的隐私文件。这时我们需要的是对文件的访问控制。

2．企业中的文件管理

企业中的重要文件资料的重要性就更大了，比如产品研发资料、项目文件、财务报表、市场规划等，保护好这些资料的安全，对企业的正常经营发展具有重要意义。

（1）员工计算机上的文件管理

对员工计算机上的文件进行管理，有利于防止员工将企业内部重要的信息资料非法复制或者外传到企业外部，造成公司的信息泄密，给企业带来经济损失和其他相关损失。近年来，企业内部人员泄密的事件层出不穷，这与企业内部对员工的管理不到位有很大的关系，特别是对计算机上的文件管理。

对员工计算机上的文件操作实行两个方面的管理：一方面将员工对文件操作的情况进行记录并上传到指定的服务器进行统一管理；另一方面严格控制员工将内部文件通过 U 盘、移动硬盘以及数码相机等外部设备将企业内部的文件复制并带出企业。

具体来讲，记录员工计算机上文件操作，记录的项目包括操作用户名、操作时间、操作类型、操作程序、操作原始文件、操作目标文件等信息，以备在必要的时候检查，对非常重要的文件，还可以选择操作前备份文件内容，比如删除计算机上的重要信息，或者删除网络上其他计算机的文件资料。

在控制方面，提供对其他计算机上的文件只读访问、禁止访问和完全访问选项设置，提供对移动存储设备文件的只读访问、禁止访问和完全访问的选项设置。有效防止员工非法利用其他计算机或者移动硬盘等非法将文件复制带出企业。

（2）文件服务器管理

对服务器上的文件按照目录分配给相关人员对应的权限，主要包括读取、写入和完全控制三种，禁止没有权限的人员对服务器上的任何文件进行访问，除此之外，在服务器端保留详细的操作记录，当出现重要的文件资料丢失时，可以及时通过操作记录查出是什么时间、什么人对文件进行什么样的操作造成的，是被删除还是改名，或者是移动，及时找出问题的原因，为及时采取措施防范同样的问题再次出现提供依据。特别是在对文件操作发生争议时，可以通过对访问日志来确认究竟是谁的责任。

5.2.2　接口管理

现在的计算机为了使用上的方便，提供了多种外设接口，比如 USB 存储设备接口、USB 打印机等。在企业中，为了防止有人利用这些接口非法将文件资料传递出去，在不影响正常工作的前提下，应该对这些外设接口进行合理的监控和管理。

1．家庭中的接口管理

家庭中计算机的用处主要在两个方面：一方面为工作上的方便；另一方面是娱乐所用。不管是哪个方面的使用都需要有合理的管理，特别是对家庭中有小孩的情况，既要让小孩通过计算机学习到更多的知识，同时也要给小孩以正确的指导，以避免其误入歧途或者给计算机的安全带来威胁。

比如对光驱的管理，防止小孩随意将从外面带回的光盘放入光驱中，因为这有可能引入病毒，另外还有可能将游戏、电影等文件复制到计算机上，然后在游戏或者看电影上花费太长的时间，以至于影响了学习。对 USB 接口的管理也是出于同样的目的。对上网的管理可以防止孩子沉溺于网络中，影响学习以及孩子的身心健康。总之，根据各种具体情况，

对计算机的各种外设接口进行合理管理，有利于孩子通过计算机学习知识、适当的娱乐，并且还有利于防止计算机影响孩子的学习和生活。

2．企业中的接口管理

随着计算机的大量普及和应用，绝大多数企业都实现了在计算机网络上办公。所以几乎所有的重要信息资料都以电子形式存放在计算机上，保护好这些重要的文件资料，避免其泄密甚至流到竞争对手那里，对企业有着重要意义。

计算机上的资料有一个重要特点就是容易复制。所以对每个员工的计算机上的外设接口进行管理，防止有人私自利用外设接口将企业内部的重要文件资料复制到企业外部是非常重要的。下面简述基本的管理流程。

（1）在通常情况下，设定员工计算机外设的初始状态为禁止使用，计算机外设包括串口、并口、USB 接口、USB 存储器、光驱、软驱（或者刻录机）、Modem、打印机、红外接口、1394 接口、网卡等。

（2）当员工计算机因为工作需要使用外设接口的时候，可以要求员工提供使用外设接口的时间、原因、申请人、批准人等信息，然后再由管理人员，开通员工计算机上对应的外设接口，并将申请信息和批准信息形成日志进行保存，方便在适当的时候进行审核，使用完成后由管理人员收回使用权限。

（3）当员工计算机上的设备使用状态（指可用或者禁止）发生改变的时候，员工计算机自动向管理人员发送消息，并指明是正常的状态改变还是非法的状态改变，服务器端以日志的方式记录员工计算机外设接口使用状态发生变化的时间以及当前所有外设接口的使用状态，必要时可以在服务器端进行检查和审核。

（4）通过将外设接口的有效管理，有效控制内部重要资料外泄的途径，保护企业的重要信息的安全，同时详细的系统日志对于及时发现信息泄密问题、及时采取保护措施以及后续信息安全工作的开展和改进都有非常重要的意义。

5.2.3 打印管理

打印文件几乎在所有的企事业单位都广泛存在，虽然这项工作非常简单，但是对其进行合理有效的管理还是很重要的。

1．打印管理的重要性

对企业中的文件打印进行管理主要是出于两个目的，一个是为了节约打印资源，防止浪费；另一个是保护企业信息资料安全，防止打印的方式泄密。不管是出于哪个目的，对文件打印进行管理都是很有必要的。

（1）在一个企业中，如果对打印没有任何约束和管理，那么对打印的浪费将是很大的，员工可能利用公司的打印资源打印一些完全与工作无关的文件，比如个人简历、个人邮件等，有的甚至用公司资源打印网上下载的小说，动辄上百页，其造成的浪费就可想而知了。

（2）更重要的是企业中的一些敏感信息，比如客户名单、核心技术资料、市场规划信息等，很有可能被企业内部人员打印出来，带出企业，甚至可能流到竞争对手那里，将对企业造成重大的经济损失和其他损失，所以很有必要对企业内部的文件打印进行管理。

2．打印管理的目标

既然打印对于企业的正常经营活动是一项必需的工作，同时合理有效的管理又是必不

可少的，那么我们应该怎样来对打印任务进行管理呢，下面提出一些基本的思路来解决这个问题。

（1）保存打印内容

完整保存每次打印任务的全部内容为 TIFF 图像格式，并可以设定分辨率。可以随时查看打印内容，这样可以非常方便查看企业内部所有打印的内容，既能有效防止打印资源的浪费，又能有效预防通过打印文件的方式泄露企业内部信息。

（2）可以重新打印以前的打印任务

完整保存每次打印任务的文档，在必要的时候，可以以 Web 方式命令打印机重新打印以前打印的文档。

（3）Web 界面管理

系统管理和报表查看全部使用 Web 界面，在任何一台工作站上均可随时管理打印资源，不需安装任何客户端程序。

系统仅需安装在服务器上，对打印客户端完全透明，对用户打印没有任何影响。

（4）集中管理、集中认证计费

任意多台打印机均可纳入管理，实现集中管理、集中认证计费，方便用户对打印资源的集中管理和成本控制。

灵活的监控方式，实现地理上分散，逻辑上集中的分布式监控方式。

多个管理员，可以分担系统管理员的相关工作。

多个角色，不同的管理员有不同的管理角色，便拥有不同的管理权限。

（5）丰富的 Web 报表

在任何一台工作站上均可随时查看报表，不用安装任何客户端程序。

多种预设的报表类型，从使用情况、打印费用、打印负荷等多方面提供图文并茂的报表，及时方便地反映出打印资源的情况。

自定义报表功能，提供最大程度的灵活性，方便用户获得重点内容。

支持将报表导出成 Excel 格式。

（6）灵活的认证计费模式

按用户名或计算机名两种认证模式，域或对等网模式的局域网都可以得到很好的支持。

支持多网域用户的账号导入和统一计费认证。

支持对不同纸张类型、彩色/黑白、单面/双面的打印情况，使用不同的费率计费。

支持按照年、季、月、周、日、固定值或不限设置用户打印配额。

通过对企业内部打印任务的监控和管理，能够有效地看出企业内部打印资源的使用情况，有效提高企业打印资源的利用率，降低打印资源的浪费，防止企业内部人员通过打印文件方式泄密企业内部重要资料。

5.2.4　用户管理

实际生活中使用 Windows 的计算机用户，大多避免不了在家庭或办公室与别人共用计算机的矛盾。合理地对计算机的用户进行配置管理，有利于保护各个用户的信息资料安全，让每个用户都像独自使用一台计算机一样。

1．多用户的特性及基本设置

由于计算机可能处于两种状态下：一种是加入到某个域中，而另一种则是单独使用或加入到某网络工作组，两种状态下多用户的特性及设置有些不同，故在以下分述。

（1）加入工作组或单独计算机的特性及多用户配置

这种情况下的 Windows XP 中，默认情况下采用欢迎屏幕登录方式，而且安装系统后默认为不需密码点击账户就可直接进入。针对 Windows NT/2000 多用户环境的主要缺陷，微软在新系统引入了共享环境中用户间快速切换的技术和远程计算机功能。在加入工作组或单机的 Windows XP 系统中，所有用户账号都被设置为可随时登录的状态。换言之，可以同时在一台计算机上打开多个账号并在已经打开的账号之间进行快速切换。而这一切只需要单击“注销”|“切换用户”即可。

在基本了解 Windows XP 多用户功能的特点后，不妨来看看多用户环境的基本设置和操作。熟悉 Windows NT/2000 的用户都知道，系统的安全建立在给不同用户分配不同权限的基础之上。而在此基础上，更进一步使用 NTFS 文件系统可通过设置文件夹的安全选项来限制受限用户对文件夹的访问，所以要实现真正意义上的安全权限控制，文件所在分区必须采用 NTFS 文件系统格式，否则多用户之间的文件安全保密就是一句空话了。所以，除非特别提出，下文均是以一台硬盘全部划为 NTFS 文件系统，装有 Windows XP Professional 中文版的计算机为例进行说明。

安装 Windows XP 的过程中需要设置登录密码，会发现这个密码在安装完系统后根本就用不上，因为系统安装后第一次启动会马上要求你创建至少一个新账户，第一个新账户默认为计算机管理员，而接下来进入系统后就是使用新创建的账户登录了。所以虽然以后的 Windows XP 正常登录界面中不会出现 Administrator 这个账户，但实际上这个账户是存在的，你只要在启动时按 F8 键选择从安全模式启动就可以看到。尽管不明白为什么微软要把这个账户隐藏起来，但很明显，要安全使用多用户环境，那么计算机的管理者首先就应注意这一账户。不少用户在安装系统时会习惯性地略过输入密码这一步，所以不要因一时疏忽而留下系统安全漏洞。当然也有补救方案，就是以安全模式登录将 Administrator 账户的密码修改或干脆删除这个账户。这样处理以后，就可以真正保证计算机管理员的权限安全性。

Windows XP 多用户功能的基本设置都可以通过“控制面板”中的“用户账户”项目完成。通常来说刚安装好的 Windows XP 系统会至少建立一个有计算机管理员权限的账号和尚未启用的 Guest（客人）账号，例如笔者手上这台机器，就有一个名为 4usoft-lmw 的计算机管理员账号和一个未启用的 Guest 账号。上文曾经提到 Windows XP 默认账户是没有密码的，所以在登录画面单击就可以进入（如果只有一个账号，Windows XP 就会自动登录），所以我们首先就要为账户添加密码，具体操作方法如下。

① 选择“开始”|“设置”|“控制面板”命令，出现“控制面板”窗口，如图 5-68 所示。

② 选择“用户管理”，双击打开“用户管理”对话框，如图 5-69 所示。

③ 选择新创建的用户账户“4usoft-lmw”，出现选择对账户操作的选择，如图 5-70 所示。

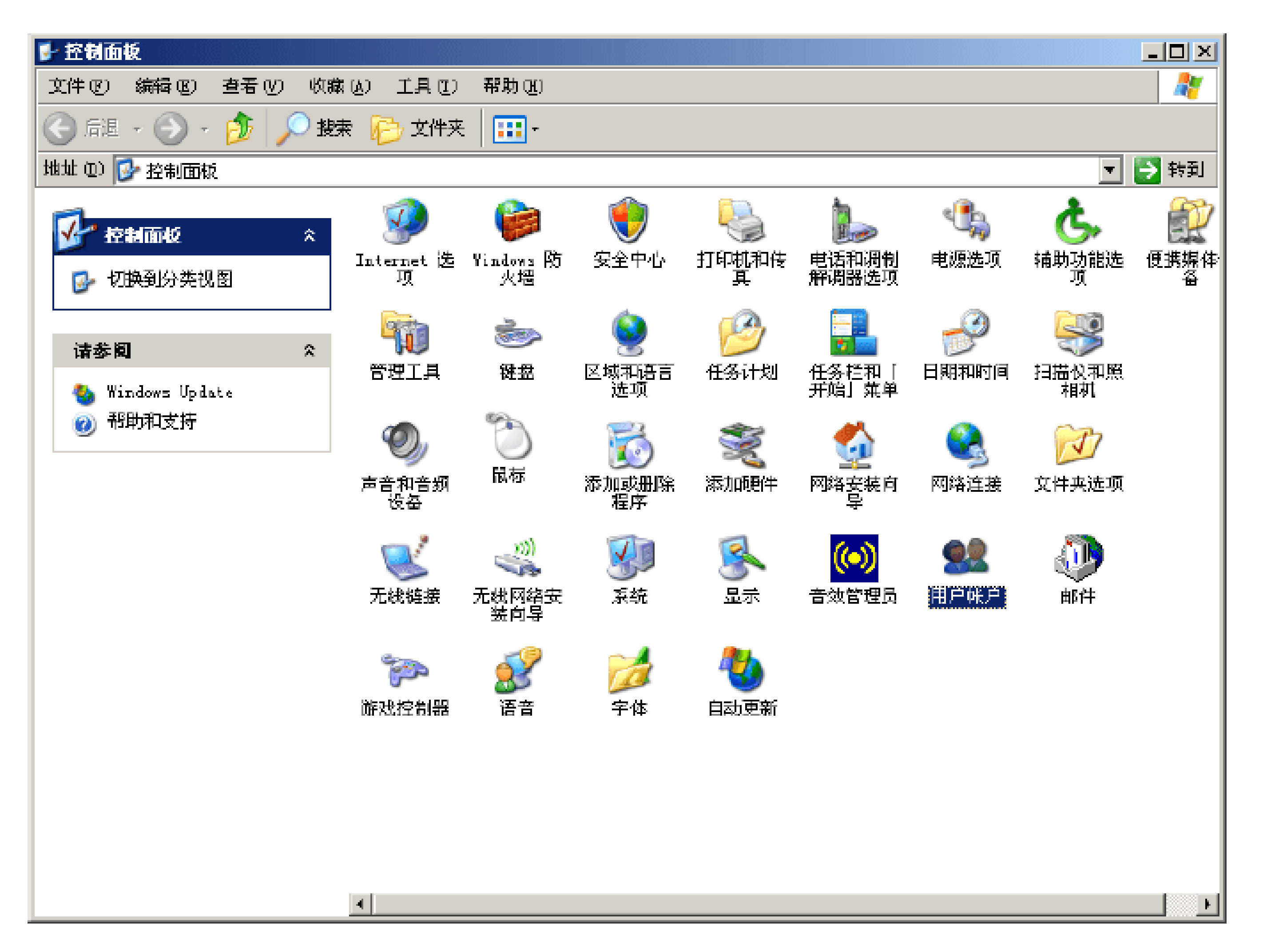


图 5-68　控制面板窗口



图 5-69　选择账户窗口



图 5-70　选择账户操作窗口

④ 单击“创建密码”，可以为“4usoft-lmw”账户设置密码，设置密码窗口如图 5-71 所示。



图 5-71 设置密码窗口

⑤ 设置完密码以后，单击“创建密码”按钮，密码就设置完成了。

由于 Windows XP 的控制面板采用向导式分类视图风格，用户设置使用起来非常简单方便，所以你不用学习都可轻易在这里完成所有的用户管理操作。

值得注意的设置是，WinXP 拥有两种方法登录计算机，默认的是“欢迎屏幕”这种快而简单的登录方法，只需单击账号并输入密码（如果有的话）就可登录，这也是 Win9X 系列用户的习惯方式；但 WinXP 还是保留了 Windows NT/2000 系列的“传统登录提示”的方式，它要求输入用户名和密码，更加安全。显然，如果你是一家人共用机器，用“欢迎屏幕”方式登录更方便，但如果是在办公室等公共场合共用机器，还是设置为“传统登录提示”的方式更为妥当。

更改登录方法只要单击“用户账户”窗口的“更改用户登录或注销的方式”在设置页面上把相应选项选中即可，如图 5-69 所示，注意这里还可以禁止“用户快速切换”功能，其需要禁止原因和登录方式的切换也是一样的，即“安全”。所以要结合自己共用计算机的具体环境来灵活设置登录方式和“用户快速切换”功能。

Windows XP 的 Administrator 账户默认模式下无法看到，也无法登录这个账号。不过你可以采用“传统登录提示”方式手动输入 Administrator 登录。那有没有办法在“欢迎屏幕”方式下以此账户登录呢？答案是肯定的。打开注册表编辑器，找到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\NTCurrentVersion\Winlogon\SpecialAccounts，打开次级主键 UserList（如果没有可自己建立），在右边新建 Dword 值，命名为 Administrator，然后修改键值为 1 即可。重新启动机器，“欢迎屏幕”方式上就出现了 Administrator 账户。

（2）加入域的计算机特性及多用户配置

加入域的计算机会受到域策略的影响。与工作组或单独计算机相比，系统不具备快速

切换用户的功能，而且只能以“传统登录提示”的方式登录，上面讲了，这样设计能有更高的安全性。同时如果计算机加入了域，控制面板中“用户账户”的设置界面也会稍有不同，更接近于 Windows NT/2000 中的设置。因为大多数用户都是在工作组或单独计算机上工作，此外域中计算机的用户设置也同样简单，这里就不详述了。

2. Windows XP 各类用户的权限

要对用户管理作出合理的设置，仅了解 Windows XP 多用户的特点和基本管理设置显然不够，我们必须要对用户管理机制做更多的了解。而由于 Windows XP 采用 Windows NT/2000 内核的用户管理安全机制，这种安全机制建立在用户权限的分配上，所以不妨来复习一下 Windows 2000 的用户分类及相应权限。

Windows 2000 中的用户分为 3 类。

第 1 类是标准用户：该用户可修改大部分计算机设置，安装不修改操作系统文件且不需安装系统服务的应用程序，创建和管理本地用户账户和组，启动或停止默认情况下不启动的服务等，但不可访问 NTFS 分区上属于其他用户的私有文件。

第 2 类是受限用户：该用户可操作计算机并保存文档，但不可以安装程序或进行可能对系统文件和设置有潜在破坏性的任何更改。

第 3 类是其他用户，又可分为 6 种：

（1）Administrator（系统管理员）——有对计算机/域的完全访问控制权；

（2）Backup Operator（备份操作员）——可以备份和还原计算机上的文件，而不论这些文件的权限如何；还可登录到计算机和关闭计算机，但不能更改安全性设置；

（3）Guest（客人）——权限同受限用户；

（4）Power User（高级用户）——权限同标准用户；

（5）Replicator（复制员）——权限是在域内复制文件；

（6）User（普通用户）——权限同受限用户。

在 Windows XP 中。用户分类、权限其实和 Windows 2000 基本一样，你同样也可以利用用户的分类来保护计算机在多用户环境下的安全。以工作组或单独计算机为例，在默认情况下，使用 Windows XP 只能够创建 2 种类型的用户：计算机管理员（Administrator）和受限用户（User），似乎管理的灵活和方便远不如 Windows 2000。其实 WinXP 只是将其他用户类型隐藏起来了，我们还是可以在控制面板里创建。这里提供 2 种简单的方法，以下以创建 Power User 账户为例，其余账户类型的创建类似。

具体操作方法如下。

（1）选择“开始”|“设置”|“控制面板”命令，出现“控制面板窗口”窗口，如图 5-68 所示。

（2）选择“用户账户”，双击打开“用户账户”对话框，如图 5-69 所示。

（3）单击“创建一个新账户”，出现创建账户窗口，如图 5-72 所示。

（4）在输入账户名称后单击“下一步”按钮，出现为新创建的用户设置属性，如图 5-73 所示。



图 5-72　创建账户窗口



图 5-73　设置创建用户属性

（5）设置用户属性为“受限”，然后单击“创建用户”按钮，新用户的创建工作就完成了。

（6）选择“开始”|“设置”|“控制面板”命令，出现“控制面板”窗口，如图 5-68 所示。

（7）选择“控制面板”窗口中的“管理工具”并双击，出现“管理工具”窗口，如图 5-74 所示。

（8）在“管理工具”窗口中双击“计算机管理”，出现“计算机管理”窗口，如图 5-75 所示。

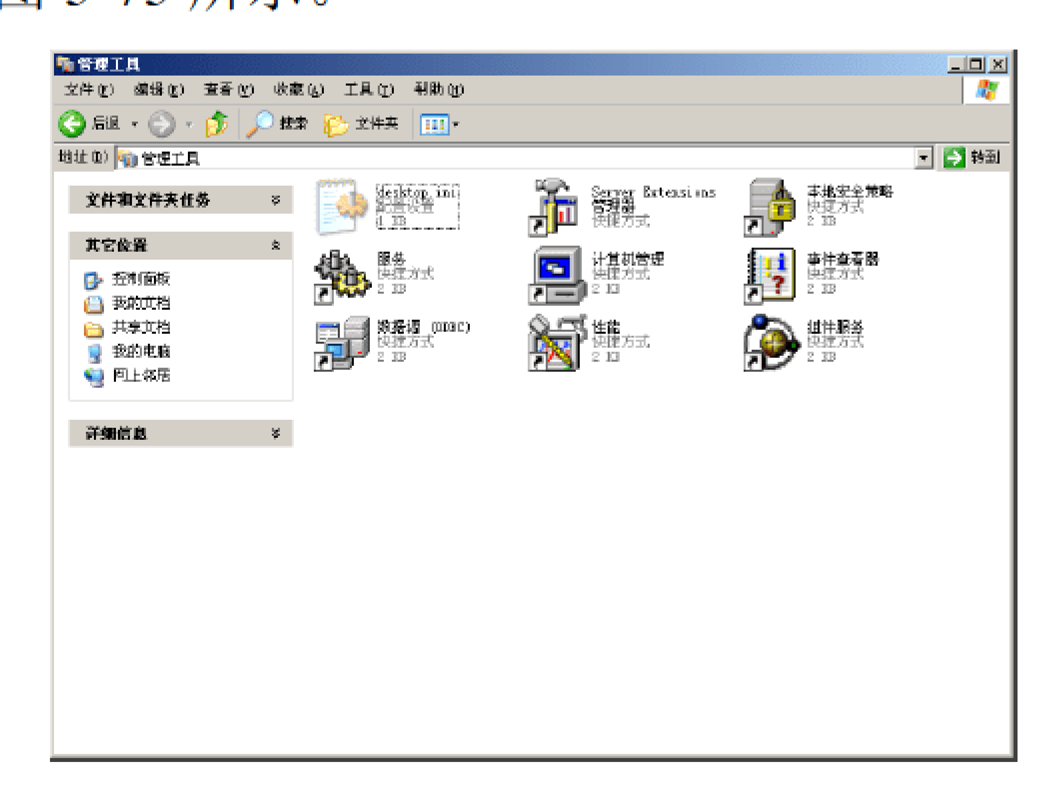


图 5-74　管理工具窗口

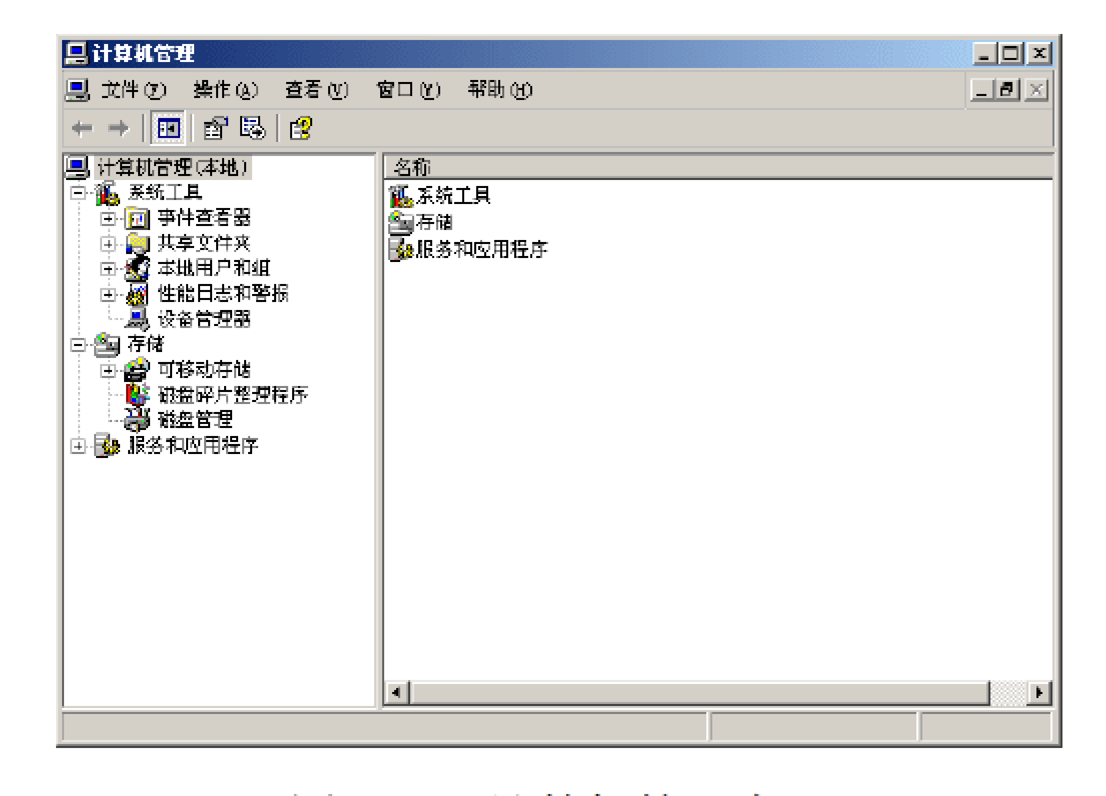


图 5-75　计算机管理窗口

（9）选择“计算机管理（本地）”|“系统工具”|“本地用户和组”|“用户”命令，再在右边窗口双击刚新建的账户 4usoft_test，出现账户属性窗口，如图 5-76 所示。

（10）选择“隶属于”选项卡，选择“隶属于”列表中的“Users”，单击“删除”按钮，将“Users”删除，然后单击“添加”按钮，出现“选择组”对话框，如图 5-77 所示。

（11）在“输入对象名称来选择”文本框中输入 Power Users，单击“检查名称”按钮，以确认输入正确无误，最后单击“确定”按钮，用户的属性设置就完成了，即 4usoft_test 就是 Power Users 组的成员了。

可以通过“计算机管理”窗口来完成添加用户并设置其属性，其操作比较简单，在这里不再介绍，留给读者作为练习来完成。





图 5-76　账户属性窗口

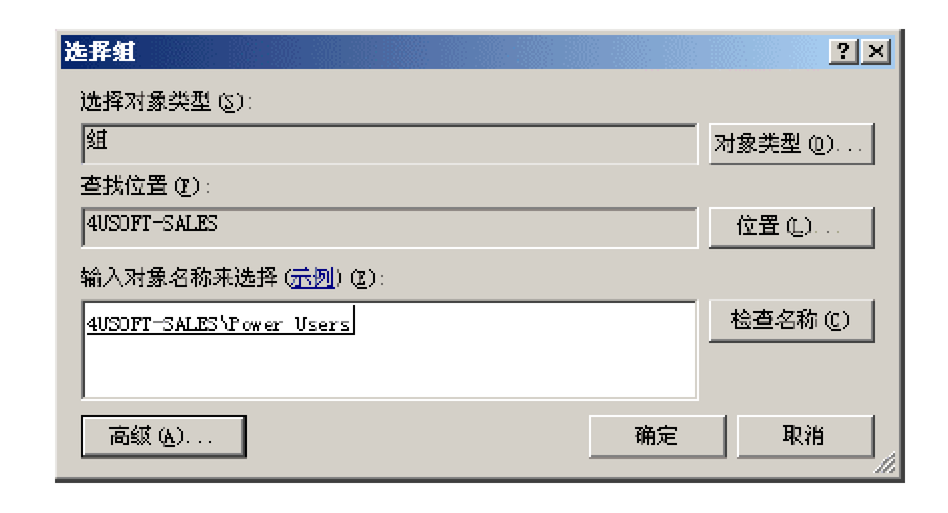


图 5-77　选择用户组对话框

这样在了解各类用户账户及其相应权限后，就可以在实际应用中对用户作相应分类，并给予相应权限，以保证各用户相互间的安全保密性和整个系统的安全保密性。最后，在进入实际设置前，如果你查看过 Windows XP 的帮助中心，肯定就会发现 Windows XP 的用户账户管理说明实际上分为单机多用户和网络多用户两种形式，下文将分别说明这两种形式下的多用户应用。

3．单机多用户的权限分配

假设有一家 3 个人共享 1 台计算机——精通计算机应用的爸爸、不关心计算机技术的妈妈和 10 岁左右的儿子。

那么相应用户权限分配可设置如下：爸爸是计算机管理员，出于安全的考虑，平常的计算机使用中不应使用管理员身份登录，爸爸为自己分配了一个 Power User 或 User 类型账户，而妈妈和儿子分别拥有自己的 User 账户。此时系统为不同的用户建立了不同用户文件夹及配置文件（用户对这个自己独有的文件夹拥有完全控制的权限）。如果使用管理员用户组的用户登录，“我的电脑”视图中可看到所有本地登录用户的“XX 的文档”文件夹，此外还有一个共享文件夹。而其他类型用户则只能在此处看到自己的“XX 的文档”文件夹，而无法看到其他登录用户的文件夹，即使直接在硬盘上能找到其他用户的相关文件夹，也不能访问文档，除非得到授权。这样就保证了除管理员外，其他用户独有文件相互之间的安全隐私性，同时也保证了普通用户在使用中不会对计算机系统造成安全危害。这时系统的日常运作基本上是安全的。

但是，随着日常的使用，爸爸发现，正处于充满好奇年龄阶段的儿子对计算机里的一切充满了探索的欲望，然而由于计算机知识不够，他常常会无意识地对硬盘上其他用户创建的文件或应用软件进行运行、修改、删除等破坏工作，又或者在硬盘的系统分区上复制大量文件而使该分区消耗殆尽等。虽然用户权限的限制不至于损害系统，但这显然对计算机的正常使用影响巨大，不关心技术的妈妈甚至有时也会犯这样的错误。这时爸爸就以管理员身份登录计算机，通过设置不同用户对文件夹的访问权限来解决这一问题。

首先，由于 Windows XP 默认的是文件简单共享方式，这种情况下无法为文件夹或文件设置访问权限，所以要去掉这一默认方式。选择资源管理器的菜单项“工具”|“文件夹选项”，进入“查看”选项卡，将“使用简单文件共享”前的复选框勾除即可。之后用鼠标右击要设置权限的文件夹（也可是整个硬盘分区），在弹出的快捷菜单中选择“属性”，并在属性对话框中选择“安全”选项卡，在这里就可添加或删除不同访问权限的组或用户。

有时我们会发现无法删除组或用户，或者由于它们的具体权限在权限列表中是灰色的而无法修改。这是因为文件夹在默认状态下继承了上级文件夹或系统分区的访问权限，所以要先去除已继承的权限才能修改。单击“安全”选项卡上的“高级”按钮，查看文件夹的高级安全设置对话框。在文件的高级安全设置对话框下方有一个“从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目”复选框，这个选项就是用来设置权限的继承，取消复选框的选择，这时又会弹出另一个对话框，如果此处选择“复制”按钮，那么该文件夹将保留上级文件夹继承下来的权限，但若以后上级文件夹权限被修改，就不会影响本文件夹；如果选择删除，就将删除所有继承自上级文件夹的权限，只保留用户单独为该文件夹设置的权限。这样就能自由设置文件夹权限了。

最后，还可限制不同用户能使用的具体磁盘空间来加强管理。具体做法是，在系统磁盘驱动器图标上单击鼠标右键，选择“属性”选项，单击“配额”选项进入配额选项面板。选择启用磁盘配额。如果你想严格控制用户可使用的磁盘空间，可选择“将磁盘空间限制为”选项，并设置相关数字。接着单击“配额项”进入具体设置，在这里可新建配额项和修改配额项。

至此，作为管理员的爸爸就可以基本保证计算机的安全和正常使用了。但要正确设置好文件的权限，还需牢记以下原则。

（1）权限是积累的——例如某个用户对一个文件有读取权限，而该用户又属于一个组，同样该组对该文件又有写的权限，那么该用户对该文件就有了读和写的双重权限；

（2）文件权限超越文件夹权限——如果某个用户对一个文件有写的权限，同时他对该文件所在文件夹只有读的权限，最后并不影响该用户对文件的写权限；

（3）拒绝权限大于一切——上面在为用户赋予权限时，都是设置其允许有什么权限，而没有设置拒绝权限，但实际上拒绝权限可以超越其他任何权限，如果你想让某个用户不能访问一个文件夹，那么你可设置该文件夹拒绝访问，这样即使该用户对此文件夹具有访问权限也不行。另外，这里给出管理员在授权时的一些有益经验：

（1）为减少工作量，尽可能为组授权，而不要为用户授权；

（2）将文件分组，如建一个文件夹专门存放资料，为该文件夹授予权限，而不必为每个文件都设置权限；

（3）实行按需分配原则，只授予用户他们需要的权限，这样可提高安全性；

（4）当你对可执行文件授权时，尽量授予读和执行权限，而不要再授予其他权限，这样可在一定程度上防止病毒的侵害。

4．单机多用户文件安全的使用事项

首先，无论你是哪一级的用户都要明白，自己的用户密码是安全的关键。如果忘记密码就会造成极大的困扰，虽然有一些技巧可恢复你的密码，但随着 Windows XP 安全性能不断升级，密码恢复将会越来越难。所以未雨绸缪为自己创建一张修复用户密码的启动软盘是个好办法：单击“控制面板”|“用户账户”，选择自己的账户进入到控制界面，之后单击窗口左上方“相关任务”下的“阻止一个已忘记的密码”选项，则进入“忘记密码向导”对话框。单击“下一步”，向导提示将一张空白的已格式化磁盘插入到软驱中，接下来向导提示输入当前密码，输入后经过几秒钟便创建完成密码启动盘了。如果有一天忘记了自己的密码，只要在欢迎登录界面单击自己账户右边的箭头，然后在弹出的提示栏中选

择"使用密码重设磁盘"，再将先前做好的密码启动盘插入软驱，按照系统提示重新设置密码就能正常登录了。

接下来将讨论，单机多用户环境下的普通用户在私人资源的安全和隐私方面的注意事项。

首先，各用户对自己的专有文件夹（即"XX 的文档"）拥有完全控制的权限，如果系统没有取消"简单共享文件"，可在文件夹属性中将某文件夹设置为"专有文件夹"以保护私人资源。若计算机取消了"简单共享文件"，就可以按上文设置用户访问权限来保护。

通过上述设置，虽然一般用户不能访问受到保护的文件，却不能阻止计算机管理员的访问，故 Windows XP 提供了 EFS 文件加密功能来解决这一问题。右击要保护的文件或文件夹，选择"属性"|"高级"，选中"加密内容以便保护数据"，两次"确定"即可；这里如果对文件夹进行加密，会多出现一个对话框，提示是加密文件夹还是该文件夹中的所有内容，加密完成后可看到被加密过的文件或文件夹名被标明为绿色。别的账号登录系统是打不开这些加密文件的，即使具有最高权限的计算机管理员也不能打开（但他可删除任何文件，包括别人的加密文件）。

作为在单机多用户环境下的管理员，首先要注意日常的运行操作不要以管理员身份登录。因为以管理员身份运行 Windows XP 容易使系统受到病毒、特洛伊木马和其他安全性威胁的侵害。例如不熟悉的 Internet 站点可能有木马代码，这些代码可下载到该系统并执行。如以管理员身份登录，木马可能会重新格式化硬盘、删除所有文件、新建具有管理访问权限的用户账户等。所以应该将自己添加到 Users 或 Power Users 组中。只有在需要执行管理任务时，如升级操作系统或配置系统参数、安装程序等，再注销并以管理员身份登录。如果觉得登录过于麻烦，也可利用临时为自己分配管理权限的技巧：（1）以安装某程序为例，在右击程序安装文件的同时按住 Shift 键；（2）在随后出现的快捷菜单中单击"运行方式"；（3）输入具有相应管理权限的用户名和密码。这种方式对于开始菜单中的应用程序同样适用。

当然，计算机管理员要好好研究控制面板里"管理工具"项目中的"本地安全策略"，这是 Windows XP 最重要的安全设置工具，系统的基本安全设置都可在这里实现，通过它你可以结合具体情况有效制订出机器的安全策略和独特技巧。例如依次选择"安全设置"|"本地策略"|"安全选项"。在右侧窗口中，双击"关机：允许系统在尚未登录的情况下被关闭"，单击"已停用"单选框并单击"确定"按钮。这样一来，就禁用了"欢迎屏幕"上的关机按钮，在尚未登录的情况下，任何人都无法执行关机操作了！仔细研究和发掘，你能创造出更多的安全管理技巧。

注意： 对于公共场合的单机多用户，如果你的私人文件极为隐密和重要，那么一定要结合其他工具软件来保护你的文件。因为 Windows XP 现有的安全性能还不足以完全保护你的文件，毕竟一些有经验的用户在配合相应工具的情况下，能轻易获取计算机管理员的权限。

5.2.5　数据备份

数据对于计算机使用者来说珍贵之处不言而喻。然而，硬件故障、软件损坏、病毒侵

袭、黑客骚扰、错误操作以及其他意想不到的原因时时都在威胁着我们的计算机，随时可能使系统崩溃而无法工作，或许不经意间您的数据以及长时间积累的资料就会化为乌有。那么，有没有办法可以避免造成这样的损失呢？答案是肯定的，这个行之有效、有时甚至是唯一的办法，就是备份！

1．细究备份技术

这里所说的“备份”仅仅限于个人数据的备份。

随着软件技术的发展，系统软件功能越来越强，备份技术也突飞猛进。专用备份程序不断推陈出新，适用程度越来越高，安全系数越来越大；高级备份软件性能越来越优，简单备份的方式也未受到淘汰；单个文件备份形态仍被看好，批量备份方式成为主流，硬盘“克隆”技术成为热门；自主的静态备份普遍被使用，自动的实时备份被越来越多的用户选择……纵观整个软件家族，用户可以选择的备份程序、方式方法越来越灵活。您可以有目的地备份单个文件，也可以有选择地复制指定文件，或者将整个硬盘压缩复制到另外的介质上；您可以让备份的数据保留计算机某一个时段完全的原貌，从而在任何时候实现该时段数据结构的原样恢复；您也可以让备份数据和硬盘数据保持同步变化，使不断变化的重要数据在发生突然变故时圆满地得到还原。

与此同时，硬件技术也在进步，适合于作为备份介质的设备越来越多，存储容量越来越大。专用的磁带机性能越来越好，光盘刻录机价格越来越低廉，Zip 磁盘、驱动器品种越来越多，小巧便携的大容量活动存储设备类型越来越丰富，可用于备份数据的网络条件越来越发达。各种存储设备的质量越来越高，便携性、可靠性都有所提升，比起当初软盘一统天下的局面，可谓天壤之别，谁都可以方便、自由地选择一款合适的备份设备。

2．抛开备份说备份

进行不同作业时，可以用于备份的方法、设备确实太多了，或许抛开“备份”才能更清晰地认识备份。系统软件可以自动为重要文件生成备份文件，应用软件提供定时自动保存、自动恢复和保存文档时自动保存备份文件的功能；备份硬件的安装使用也越来越简便……但有些用户对于便利的软件设置和硬件设备却置之不理，等真的受到惩罚时，才万般无奈地求助于他人，或者摸索着用数据恢复程序侥幸地找回一部分丢失的数据，但是损失已经不可避免。其实，备份是件很简单的事情，只要构建一个理想的备份方案就行了。这个理想的备份方案，简而言之就是“四个一”政策：一套清晰的思路，一种可行的方法，一台好用的设备，一个强劲的软件。

下面，我们从 4 个方面分别介绍几种备选方案，您可根据自己的实际情况，恰当组合。

3．一套清晰的思路

哪些文件必须备份、哪些文件不一定要备份；哪些可以本地备份、哪些必须异地备份；哪些应该动态备份、哪些应该静态备份；哪些应该活备份、哪些必须强制性地死备份……这些问题一定要做到心中有数。

认识备份术语 了解备份方法

硬件级问题：选择备份文件用的存储设备和位置。 软件级问题：选择备份程序并充分挖掘、利用其功能。

本地备份：在本机硬盘的特定区域备份文件。

异地备份：将文件备份到与计算机分离的存储介质，如软盘、Zip 磁盘、光盘以及存储

卡等介质。这是备份的硬件级问题。

活备份：备份到可擦写存储介质，以便更新和修改。

死备份：备份到不可擦写的存储介质，以防错误删除和别人有意篡改。这还是备份的硬件级问题。

动态备份：利用软件功能定时自动备份指定文件，或文件内容产生变化后随时自动备份。

静态备份：为保持文件原貌而进行人工备份。这是本地备份的软件级问题。

对于每一个计算机用户来说，全部文件可分为 4 个类型。

（1）安装系统软件和应用软件形成的文件：计算机借助于它们正常运行、实现功能。这些文件不一定非要备份，因为这类文件可以通过重新安装软件再次得到。但是，有选择地备份系统软件中保证最低运行的重要的文件(如 Windows 的注册表文件以及软、硬件配置信息和用户信息)以及应用软件中的个人配置信息文件（如个人模板）可以有效地减少重新安装的麻烦。这类文件只进行本地活备份即可，不过，一定要进行静态备份，因为这类文件的价值在于其原始性，动态备份可能会把改变的甚至产生错误的文件保存为最终备份。

（2）从网络等媒体上复制的文件（如下载的软件、媒体上的文献等)： 这类文件有些可以复得，有些过期则会消失。对于您来说，下载后就成了唯一的，所以，一定要备份，重要的还要异地备份，当然是静态备份，因为复制它的目的一般是使用而不是进行修改。

（3）计算机自动生成或用户添加形成的个人信息（如输入法词库、网页收藏夹等）：这类文件一旦丢失，虽可重新建立，但却要花费很大精力重新组织，因此一定要备份。不过，它们是随时都在更新变化的，所以最好进行本地动态的活备份，以便随时恢复到最新状态; 当然，在一定阶段做一个异地的死备份也是必要的。

（4）纯属自己积累和编辑的文件（如通信簿、电子邮件、自己编辑的各种文档）：这是自己的劳动果实，也是独一无二、无法复得的，应该采用动态备份，随时记录最新形态；取得阶段性成果后要做静态的异地备份，以便万一出错时进行恢复；文件完成后，做至少 2 个死备份，以防备份丢失、被篡改，或者因存储介质损毁而不可使用。

当然，这些不是教条的，明晰的思路还应该是善于应变的。比如 Windows 注册表在系统运行过程中会随时被有意无意地修改，所以有必要进行动态备份；但如果不保留一个最初的完好备份，就可能在最需要时找到一个带有致命错误的注册表。所以，综合应用多种备份方法才是合理的。

4. 一种可行的方法

（1）选择备份工具

首先，好的备份硬件才能使良好的备份方案有的放矢。其次，要选择一个功能完善的备份程序，才能使软件级的备份方法得以实现。对于正常运行的系统，备份程序在后台作业，以保持数据同步(原始文件和备份文件随时保持一致)的动态备份是比较理想的备份方案。

（2）选择备份方法

选好备份硬件和动态备份程序后，还要考虑备份方法。进行文件还是文件夹备份？是否过滤？如何过滤？是否采用压缩备份方式？备份文件是否易于恢复？是否选择文件数据同步？如果选择数据同步，还应考虑原始文件出错的因素，有些非法操作会造成原始文件

出现非法代码而不能打开，若完全采用动态备份，原始文件和备份文件两者完全同步，备份文件也将不能使用。因此，根据自己的实际情况，选择可行方法是非常重要的。

（3）选择保存方法

备份文件是为了在发生意外时能够恢复文件，如果备份文件存放不好，所有的努力都可能前功尽弃。比如 CIH 病毒侵害计算机，往往会吞噬全部硬盘数据，如果仅仅在本地动态备份，备份文件也在其破坏范围之内。还有一些人为的破坏更甚于此。要避免此类情况，就必须采用异地备份。而异地备份的存储介质也可能遭人篡改，这就需要死备份。然而，异地死备份就达不到动态备份的目的。因此，在动态备份的同时，适当的时候做一次异地备份是最值得推广的安全方案。

（4）选择文件格式

用不同程序、不同方法备份的文件，恢复的方法也是不同的。一般来说，基于 Windows 系统的备份程序产生的特殊格式的备份文件仍要在 Windows 中恢复，尤其是压缩格式的备份文件。这对个人文档备份来说不存在问题，而对系统文件的备份就不合适了。对系统文件的备份，一定要保存成在 DOS 环境可以直接拷贝的类型或可以在 DOS 中解开的压缩格式，因为在系统无法启动时总要使用这些备份。

5. 一台好用的设备

备份离不开存储设备和介质。目前，可以用来备份的设备很多，除软盘、本地硬盘外，CD-R、CD-RW 光盘、Zip 磁盘、活动硬盘、移动存储设备以及磁带机等都可以很方便地买到。此外，Internet 还给用户提供了网络备份的新途径，尤其是一些免费空间很值得我们予以关注。

软盘是最常见的备份介质。不过，软盘容量很小，备份少量数据尚勉强可为，对大量数据则无能为力。再则，软盘安全性差、容易损坏，专业备份不值得考虑。

光盘是不错的备份介质，它容量大、便于保管和携带，安全性也较高，是死备份的唯一选择。

Zip 磁盘的容量大，容易实现异地备份。其性价比较高。在不同场合文件交换量较大的用户可以首先考虑选择它作为备份设备。

经常需要进行移动作业的用户可以把中、大容量的活动硬盘作为备份设备的首选，虽然价格有些贵，但除备份功能之外，它还能让您随身带着系统和数据库。对拥有数码相机、数码摄像机的用户而言，移动存储卡或记忆棒也可以暂时借以备份数据。磁带机是一种较原始的数据载体，但新型产品性能已经相当完善，对于从事数据生产的专业用户还是值得选择的。

如果淡化异地备份的重要性，任何人都可以把本地硬盘作为最佳备份设备。在硬盘上建立一个占总容量 20%左右的分区专用于备份文件，备份、还原都很方便，效率最高、速度最快、单位容量/价格比最高。其弊端是这个分区无法从计算机系统中分离出去，备份文件仍处于 CIH 等极具破坏力的病毒控制之下。对此，您可以用文档压缩备份、建立多级目录、隐藏文件等方法缓解潜在的危险。此外，您还可以购买一个价格较低廉的小硬盘专做备份，平时，在 CMOS 中把它设为从属硬盘隐藏起来，需要备份和恢复文件时，对 CMOS 做简单设置即可激活它。

习题

1．下载一个系统安全补丁，并安装好。
2．给系统做一个备份。
3．下载并安装一个反间谍软件。
4．将计算机建立成两个用户，并配置好权限。

第 6 章　局域网安全管理

教学提示

伴随着计算机和网络的迅猛发展和广泛应用，作为包含着网络设备与信息系统的局域网环境，其安全问题也日益突出，本章在分析局域网安全隐患的基础上，探讨了局域网安全系统建设中需要重点考虑的几个方面，并对局域网安全体系的结构及相关安全技术进行了讨论。

针对大型局域网的网络安全解决方案，应该包括原有网络系统分析、安全需求分析、安全目标的确立、安全体系结构的设计等。方案的实施应以不影响企业局域网当前业务为前提，实现对企业局域网全面的安全管理。方案的内容应该包括如下内容：

- 将安全策略、硬件及软件等方法结合起来，构成一个统一的防御系统，有效阻止非法用户进入网络，减少网络的安全风险。
- 定期进行漏洞扫描，审计跟踪，及时发现问题，解决问题。
- 通过入侵检测等方式实现实时安全监控，提供快速响应故障的手段，同时具备很好的安全取证措施。
- 使网络管理者能够很快重新组织被破坏了的文件或应用，使系统重新恢复到破坏前的状态，最大限度地减少损失。
- 在工作站、服务器上安装相应的防病毒软件，由中央控制台统一控制和管理，实现全网统一防病毒。

通过对本章的学习，应当充分掌握局域网安全相关知识，理解局域网中可能存在的安全威胁并能清楚其产生的原因，知道其危害严重程度并掌握解决问题的思路和方法。

教学重点

- 局域网的各种安全威胁产生原因。
- 局域网的各种安全威胁的危害严重程度。
- 局域网的各种安全威胁的解决方法。
- 局域网网络安全需求分析和安全目标。
- 局域网网络安全方案的总体原则。
- 局域网网络安全体系结构。
- 局域网网络安全技术。

6.1　局域网概述

随着计算机技术和网络技术的不断发展，建立在其上的应用不断丰富，以前高昂的价格不断降低，逐步被人们所接受，使得几乎所有的政府机关、学校、医院、银行、商业企业等单位都建立起了自己的局域网，将原有业务尽量用计算机网络来完成，主要的目的是

提高效率，降低成本。当然，计算机网络有其自身的复杂性和特点，如果没有进行合理有效的管理，也可能给单位带来各种程度的损失，甚至是灾难，而且这样的实例已经多次发生过，所以网络安全问题日益成为人们关注的焦点。

据统计，超过 50%的网络及信息安全问题源于内部人员所为，可见管理好局域网在整个网络信息安全体系中具有重要的地位。由于局域网是一个由网络设备与信息系统组成的复杂环境，连接便捷、应用系统多、重要数据多是其显著特点，如果疏于对局域网的安全防范，那么就极易出现应用系统被非法使用、数据被窃取和被破坏等情况，因此注重局域网安全系统建设、有效防范源自局域网内的安全问题具有重要意义。

6.1.1　网络概况

在对现有网络或者是新建立的网络规划网络信息安全解决方案时一定要考虑网络本身的基本情况，只有在了解网络基本情况的基础上才能够规划出适当的解决方案。

1．网络基本情况

（1）网络规模，比如有多少台计算机，多少个交换机，多少个路由器。

（2）网络距离，是在同一房间还是分布在不同房间，是在同一楼层还是分布在不同楼层，是在同一栋建筑物还是不同建筑物，是否需要跨越因特网。

（3）网络速度，是十兆、百兆还是千兆或者更高。

（4）是否与 Internet 连接，连接的方式如何，是选择拨号连接，还是专线连接，速度如何，选择多少兆带宽。

（5）是否对外提供 Web 服务，如直接对外发布信息或者发送电子邮件，提供网上订货、网上付款等电子商务应用。

（6）网络的主要用途包括哪些，如生产、研发、办公、财务、销售等。

通过对网络结构、连接方式、网络规模、网络应用等基本情况的了解，有利于了解网络存在的各种潜在安全威胁，为有针对性地提供网络信息安全解决方案并解决各种安全问题提供依据。

2．网络结构规划

企业局域网通常按照其功能特点可以分为三个区域，即 Internet 区域、内部网络、公开服务器区域。

（1）Internet 区域是指可以直接和 Internet 连接，进行对外邮件发送、资料查询、下载文件、即时通信等。

（2）根据安全要求层级的需要，内部网络不能和 Internet 连接，只提供企业内部信息交流。为进一步提供企业内部网络结构上的安全性，内部网络又可按照所属的部门、职能、安全重要程度等分为许多子网，比如财务子网、领导子网、办公子网、市场部子网、中心服务器子网等。

（3）在安全方案设计中，基于安全的重要程度和要保护的对象，可以在三层交换机上直接划分出多个虚拟局域网（VLAN），如中心服务器子网、财务子网、领导子网、其他子网，虚拟局域网较之传统子网有更多的灵活性和可控性。

（4）不同的局域网分属不同的广播域，由于财务子网、领导子网、中心服务器子网属于重要网段，因此在中心交换机上将这些网段各自划分为一个独立的广播域，而将其他的

工作站划分在一个相同的网段。

（5）公开服务器区域是指专门对外提供 Internet 服务的计算机，提供的服务包含网上订货、信息发布、网上交流等，这些计算机应该与内部网隔离，避免来自外部的攻击而影响到内部网络的安全。

6.1.2 网络应用

企业建立局域网的出发点和归属都在于应用其提供的功能上面，只有局域网有效提供了其应该有的功能以后，企业对其所做的所有投入才有意义，那么我们来讨论一下企业局域网会给企业带来哪些应用呢？

1．文件共享

文件共享是企业局域网的一项基本功能，也是企业最基本的一项应用。传统的纸质文件需要人工传递，现在基于计算机的电子文件只需要通过共享，就可以让局域网内相关的每个用户看到，无疑通过这样的方式提高了工作效率，同时降低了成本。

2．办公自动化

作为提高企业办公管理效率的基础平台，近年来，办公自动化系统受到各企业高度重视，他们纷纷构建起适合于自身应用特色的办公自动化系统，从而逐步提高企业的工作效率并提升管理质量。

通过为企业构建高效实用的企业办公系统，使企业内实现高效率信息沟通联络、网络协同无纸化办公；帮助企业最终实现规范管理、信息资源高效传递；使企业从彼此独立被动的混乱管理模式转向一体化、信息共享的统一管理模式。

3．WWW 服务

企业通过内部 WWW 服务的方式进行信息发布，在内部网站上进行信息交流，通过企业内部网站进行信息交流，有效防止直接和外部网络连接的风险，同时也减小了内部人员通过外部网络泄密内部信息的可能。

4．电子邮件服务

电子邮件是人们使用最广泛的一种信息交流方式，企业通过内部网络系统提供邮件收发服务，使企业内部人员在免受外部安全威胁的环境下能够通过电子邮件进行快捷方便的信息交流。

5．文件数据的统一存储

在一个企业中，各种数据分散存储在网络的各个角落，比如财务数据存储在财务部门的计算机上，市场数据存储在市场部门的计算机上，销售数据存储在销售部门的计算机上等等，这些数据对于企业的日常经营管理和发展都具有重要作用，保证其安全性是必需的。通过企业内部网络，可以把这些数据统一存储到专门的计算机上，然后进行统一管理和保护，这也是企业局域网所提供的一个重要功能。

6．二次开发

企业局域网的发展和完善是一个逐步的过程，建立在其基础上的应用和发展也是一样的，所以建立企业网络的时候就要考虑到将来一段时间的发展情况，为其保留一定的扩展余地。软件系统一般将这种情况称为二次开发。

7. 提供与 Internet 的访问

为了方便企业内部人员及时获取外部信息，查询工作所需资料以及方便地和外界保持联系（比如市场人员和销售人员与供应商、合作伙伴以及客户的联系），企业局域网为他们提供直接访问 Internet 的权限。

8. 对外信息发布

企业通过公开服务器对外发布企业信息、收发电子邮件、网上订货、网上交流等，同时也搜集外界对公司的反馈意见，形成一个企业对外交流信息平台。

6.1.3 网络结构特点

在分析企业局域网的安全风险时，应考虑到网络的特点，因为它们都与网络信息安全息息相关，是否能够针对这些情况做好安全管理工作，直接关系到整个企业局域网的安全。

1. 网络与 Internet 直接连接

在进行安全方案设计时要考虑与 Internet 连接的有关风险，包括可能通过 Internet 传播进来病毒，黑客攻击，来自 Internet 的非授权访问等。

2. 网络中存在公开服务器

由于公开服务器对外必须开放部分业务，因此在进行安全方案设计时应该考虑采用安全服务器网络，避免公开服务器的安全风险扩散到内部。

3. 内部网络中存在许多不同的子网

不同的子网有不同的安全性，因此在进行安全方案设计时，应考虑将不同功能和安全级别的网络分割开，这可以通过交换机划分 VLAN 来实现。

4. 网络中有哪些应用和服务器

在应用程序开发时就应考虑加强用户登录验证，防止非授权的访问等，对于安全性要求较高的应用软件（如财务软件）可考虑数据的加密传输。了解企业中的各种应用的特点以及安全性要求，特别是存储企业重要信息的文件服务器、应用服务器、数据库服务器等的安全需要特殊处理。

6.2 安全评估

安全评估是依据安全管理的方针和保证程度的要求，综合考虑组织特性、地理位置、资产和技术等因素，充分利用各类信息（如威胁信息、脆弱性信息和影响信息等）对网络及信息系统的安全状况给予评价，确定由安全问题带来的风险程度，并选择合适的控制目标和控制方式。

6.2.1 网络安全为何会失败

经过我们自己的亲身体验和媒体的报道，我们认识到了网络安全的重要性，也希望采取一些措施来解决网络安全问题。但是往往会发现，我们虽然采取了网络安全的防范措施，但是却没能达到理想的效果，这就是这里所说的网络安全失败。那么有哪些原因会导致网络安全失败呢？下面我们将对主要的几种情况进行分别讨论。

（1）人的意识

虽然网络安全意识比起以前有了较大提高，但是还远远不够，比如有的人计算机不设置密码或者设置非常简单的密码，有的人不安装杀毒软件和防火墙软件，有的人随意从外面带来的光盘或者移动硬盘复制文件到自己的计算机等，这些都是安全隐患，虽然不一定会造成安全问题，但是这些行为都会增加安全隐患。

提高安全意识是解决网络安全问题的第一步，如果没有足够的安全意识，总是心存侥幸或者怕小的麻烦，就有可能带来更大的危害，甚至是重大损失。只有人们的安全意识提高了，行为得到规范以后，安全问题才可能得到很好的解决。

（2）策略因素

安全策略是一种处理安全问题的管理策略的描述。策略要能对某个安全主题进行描绘，探讨其必要性和重要性，解释清楚什么该做什么不该做。安全策略应该简明，在生产效率和安全之间应该有一个好的平衡点，易于实现、易于理解。安全策略必须遵循三个基本概念，即确定性、完整性和有效性。

从上面可以看出，安全策略既要考虑到细节，又要照顾到全局，对具体某个问题的处理也要同时考虑到方便性和安全性（因为方便性和安全性往往是矛盾的）。尤其是对于一个大型的企业网络系统而言，没有系统、完整的安全策略是根本无法有效解决网络安全问题的，这就要求在安全策略上面多下工夫。

（3）硬件或软件配置错误

计算机硬件或者软件提供多种配置选择是为了满足多种不同的需要，提供了一定程度的灵活性，也正是因为如此，如果对各项配置不是很清楚其功能和意义的话，很有可能出现配置错误的情况，结果使之前所做的安全投资完全没有意义了，从而导致网络安全问题。一个很明显的例子就是计算机上虽然安装了防火墙，可是觉得老是弹出安全警告，所以就把防火墙设置为全部通过，结果防火墙就形同虚设了。

（4）不充分的假设

实际上，我们对多数网络安全问题的处理基本上都是基于假设来做的，只有极少数是自己实际经历过的。即使对于我们所经历过的网络安全问题，也只是经历了其中的部分情况，不太可能经历全部情况。所以我们在做安全问题假设的时候很有可能考虑不周，这也是引发安全问题的一大原因。

（5）无知

计算机网络安全知识广泛而且复杂，即使对于专业的网络安全人员也不可能面面俱到地了解，对于普通的计算机使用者来说，就更不可能完全依靠自己来解决相关的安全问题了，所以需要平时不断地学习和丰富网络安全知识，在必要的时候多向相关专业人员请教，而不是跟着感觉走。

（6）未能保持最新

系统软件和应用软件都是一个逐步完善的过程，特别是计算机操作系统，随着时间的推移，经常会有新的漏洞被发现，开发厂商会对新的漏洞开发相应的补丁程序，所以对计算机用户而言，也需要及时安装最新的补丁程序，而不是等到已经收到安全威胁以后再去想办法解决。

6.2.2　为何要执行安全评估

我们的网络是否安全？如何知道我们的网络是安全的？要回答这两个问题，唯一的方法就是通过安全评估。执行安全评估就是要确定网络是否安全，都存在哪些安全隐患，需要采取什么样的措施来予以解决，主要包括以下几个方面。

（1）提供一个基准来帮助改善安全性

由于计算机网络系统的复杂性，绝对的安全往往是不存在的，这就要求我们根据以往的经验来确定一个安全的标准，并对目标网络的各种安全状况进行审查，对于不符合安全要求和规范的项目，积极采取有效措施，消除安全隐患，只有消除了不符合安全标准的项目，才能提高整个网络的安全性。

（2）查找配置错误或缺少的安全更新

通过安全评估，及时找出系统中存在的配置错误以及缺少的安全更新，因为这些都是系统存在的安全隐患。

（3）揭露出组织安全中的意外缺陷

计算机网络是一个复杂的系统，如果没有系统全面地进行检查过，难免会存在没有考虑到的安全问题，这些问题通常在发生安全事故以后才被发现。而安全评估要做的就是通过对网络系统进行全面细致的检查，发现潜在的安全威胁，将安全问题提前解决。

（4）确保符合法规

在一些特殊的部门中（比如银行、政府部门和军队等），对计算机信息安全保密具有严格的规定和要求。但由于种种原因，可能存在没有严格按照规定执行，这将可能造成网络系统的严重安全威胁，所以需要通过安全评估来发现这些问题，并解决这些问题。

6.2.3　规划安全评估

网络安全评估是一个系统的过程，为了做好网络安全评估工作，通常将整个过程划分为以下几个步骤，下面我们对这几个步骤做一个简要的说明。

（1）预评估

预评估可以看作是网络安全评估的准备工作，需要确定的内容包括范围、目标、时间线、基本规则等。范围是指需要进行安全评估的网络范围，比如是整个网络还是部分子网等；目标是指通过此次评估需要解决哪些安全问题，比如为了确认某个漏洞是否已经被修复；时间线是指在网络上进行安全评估的时间范围，比如是选择休息时间还是工作时间；基本规则是指使用什么样的方式和方法来达到安全评估的目的，比如是直接通过扫描还是突破测试。

（2）评估

在做好评估准备工作以后，就可以开始选择评估技术，比如扫描技术、网络攻击技术、入侵检测技术等，然后执行评估，组织评估结果。

（3）准备结果

将评估过程中发现的缺陷所带来的风险进行评估，制定补救计划，确定尚未纠正的漏洞，确定一段时间内的网络安全改进，将所有这些内容形成网络安全评估报告。

（4）报告评估结果

向相关负责人提供评估报告，为领导在改进网络安全方面提供依据，以便及时采取行动，修正已经发现的网络安全漏洞，并为下一次安全评估做准备。

6.2.4 安全评估范围

确定安全评估范围是安全评估准备工作的重要组成部分之一，只有确定了安全评估的范围，安全评估工作才具有现实意义，下面以一个具体的例子来说明。

（1）目标

如运行以下操作系统的所有服务器，Windows 2000 Server，Windows 2003 Server，范围描述中指出了两个条件，一个是操作系统的版本，另一个要求是服务器。

（2）区域范围

如以下字段中的所有服务器，192.168.0.1/24，192.168.1.1/24，区域范围描述确定了是两个网段中的计算机，而不是整个网络。

（3）时间线

如扫描将在 6 月 3 日到 6 月 10 日的非重要工作时间进行。时间线指定了两个条件，一个是执行评估的时间范围，另一个是执行评估与工作重要程度的关系。

（4）要扫描的漏洞

比如 RPC-over-DCOM 漏洞（MS03-026）、匿名 SAM 枚举、启用 Guest 账户和本地 Administrator 组中多余 10 个的账户，确定了需要扫描的漏洞是这些，而不是其他的。

6.2.5 安全评估目标

确定安全评估范围是安全评估准备工作的重要组成部分之一，只有明确的目标才能事半功倍。下面我们举例说明。

（1）项目目标

将对子网 192.168.0.1/24 和 192.168.1.1/24 中所有运行 Windows 2000 Server 和 Windows 2003 Server 的计算机进行扫描，以查找以下漏洞，并按照所述方式加以修正。

（2）漏洞及补救措施如表 6-1 所示。

表 6-1　漏洞与补救措施

漏　洞	补 救 措 施
RPC-over-DCOM 漏洞（MS03-026）	安装 Windows 安全更新 03-026 和 03-39
匿名 SAM 枚举	将 RestrictAnonymous 配置为 2（在 Windows 2000 Server 上）或 1（在 Windows 2003 Server）
启用 Guest 账户	禁用 Guest 账户
本地 Administrator 组中多余 10 个的账户	将管理员组中的账户数减至最小

6.2.6 安全评估的类型

网络安全评估主要包括以下三种类型，分别针对三种不同的安全问题，下面做一个简单的介绍。

（1）漏洞扫描

漏洞扫描侧重于已知缺陷，通过专门的漏洞扫描工具来完成，可以自动进行，不一定需要专业知识。

（2）突破测试

突破测试侧重于已知和未知的缺陷，通过模拟攻击者对网络进行攻击，不但需要工具的配合，还需要测试者具有丰富的攻击知识以及熟练的操作技能，但是攻击测试需要取得相关单位和部门的同意后才能进行，否则非法的攻击是被禁止的，甚至会承担法律责任。

（3）IT 安全审核

安全审核侧重于安全策略和过程，主要是检查安全策略是否如实落实到位以及是否存在违背安全规范的行为，用于给行为规范提供证据。对于违反安全策略的行为予以制止和纠正，并追究相关人员的责任，避免类似情况的再次发生。

6.2.7　使用漏洞扫描来评估网络安全

漏洞扫描是常见的网络安全评估技术之一，使用漏洞扫描来评估网络安全的基本思路是先假设系统存在某些漏洞，然后再进行扫描确认，最后指出改进方法，一般需要执行以下几个步骤。

（1）检测漏洞

检测漏洞就是对假设存在的漏洞进行确认的过程，即使用扫描工具对网络进行扫描，以确认假设的漏洞是否确实存在。

（2）为找到的漏洞分配风险级别

通常情况下，对于一个网络系统都会存在多种多样的漏洞，尤其是对于管理还不够完善的计算机网络系统更是如此，如果每个安全漏洞都同样对待的话，一方面没有必要，另一方面也是不合理的，所以需要为各种安全漏洞确定一个风险级别，以确定其重要性和危险性，为后续采取安全措施的优先次序提供参考。

（3）确定尚未纠正的漏洞

网络安全漏洞的发现和纠正都是一个循序渐进的过程，所以我们发现的漏洞有的可能在之前被修复了，而有的却没有，我们需要进一步确定。

（4）确定一段时间内的网络安全改进

既然知道了网络中存在哪些安全漏洞，也清楚了它们的重要性和危险性，那么就应该指定纠正和改进的具体方法和措施了，只有对发现的、尚未纠正的措施进行纠正，网络安全才能得到切实解决。

6.2.8　使用突破测试来评估网络安全

突破测试也是常见网络安全评估的主要技术之一，突破测试就是模拟网络攻击，从这个过程中发现网络的安全漏洞，一次成功的突破测试的步骤包括：

（1）确定攻击者将最可能如何着手攻击网络或应用程序；

（2）找到网络或应用程序防御中的缺陷区域；

（3）确定攻击者可能会如何利用缺陷；

（4）找到可能被访问、更改或破坏的资产；

（5）确定攻击是否被检测到；

（6）确定攻击痕迹的特征；

（7）提出防止此类攻击的建议。

6.2.9 安全审核的组成部分

安全审核贯穿于安全评估的整个过程，目的在于确保安全评估过程的前后一致性。即安全策略中要求做的事情，都在后续的过程中得到了明确的体现，而且在执行的时候做了切实的执行。

安全审核体现在策略、过程、技术、实施、文档和操作中，在这些步骤中，将每个步骤所应该做的和已经做了的进行比较，确认存在的差距和不足。安全审核就在于找出安全评估过程中的不足之处，使得整个安全评估过程能够更加完善、更加真实。安全评估中一个重要的方面不是没有想到，而是想到了但是没有采取措施，即通常的前后不一致，通过安全审核，可以有效地发现这些问题并加以解决，这是安全审核的一个重要作用。

6.2.10 报告安全评估结果

通过安全评估，发现了网络中存在的安全漏洞以及危险程度，确定了安全漏洞的解决方法，现在需要对这些内容进行整理，形成一个安全评估报告。具体的步骤如下。

（1）定义漏洞；

（2）记录缓解计划；

（3）确定应在何处进行修改；

（4）指派实施已批准建议的责任；

（5）为下一次安全评估建议一个时间。

安全评估是实施内网安全系统建设的基础，在评估过程中可以深刻理解内网安全管理的目标、全面掌握内网安全现状、及时发现各类安全隐患。

6.3 网络系统安全风险分析

针对企业局域网中存在的安全隐患，在进行安全方案设计时，下述安全风险必须要认真考虑，并且要针对面临的风险，采取相应的安全措施。下述风险由多种因素引起，与企业局域网结构和系统的应用、局域网内网络服务器的可靠性等因素密切相关。下面列出这类风险因素。

网络安全可从以下 5 个方面来理解：

（1）网络物理是否安全；

（2）网络平台是否安全；

（3）系统是否安全；

（4）应用是否安全；

（5）管理是否安全。

针对每一类安全风险，结合企业局域网的实际情况，我们将具体地分析网络的安全风险。

6.3.1　物理安全风险分析

网络的物理安全的风险是多种多样的。

（1）网络的物理安全主要是指地震、水灾、火灾等环境事故；

（2）电源故障；

（3）人为操作失误或错误；

（4）设备被盗、被毁；

（5）电磁干扰；

（6）线路截获。

真正做好物理安全风险的防范工作，比如采用高可用性的硬件、双机多冗余的设计、机房环境及报警系统、提高安全意识等。做好物理安全风险的防范工作是整个网络系统安全的前提，在企业局域网内，如果网络的物理跨度不大，只要制定健全的安全管理制度，做好备份，并且加强网络设备和机房的管理，这些风险是可以避免的。

6.3.2　网络平台的安全风险分析

网络平台的安全涉及到网络拓扑结构、网络路由状况及网络的环境等。

（1）整个网络结构和路由状况

安全的应用往往是建立在网络系统之上的。网络系统的成熟与否直接影响安全系统的成功建设。在企业局域网络系统中，使用一台路由器，用作与 Internet 连接的边界路由器，网络结构相对简单，具体配置时可以考虑使用静态路由，这就大大减少了因网络结构和网络路由造成的安全风险。

（2）公开服务器面临的威胁

企业局域网内公开服务器区（WWW、EMAIL 等服务器）作为公司的信息发布平台，一旦不能运行或者受到攻击，对企业的声誉影响巨大。同时公开服务器本身要为外界服务，必须开放相应的服务；每天，黑客都在试图闯入 Internet 节点，这些节点如果不保持警惕，可能连黑客怎么闯入的都不知道，甚至会成为黑客入侵其他站点的跳板。因此，对规模比较大的网络，网络管理人员对 Internet 安全事故做出有效反应变得十分重要。有必要将公开服务器、内部网络与外部网络进行隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。

6.3.3　系统的安全风险分析

所谓系统的安全显而易见是指整个局域网网络操作系统、网络硬件平台是否可靠且值得信任。

对于中国来说，恐怕没有绝对安全的操作系统可以选择，无论是 Microsoft 的 Windows NT 或者其他任何商用 UNIX 操作系统，其开发厂商都可能存在其 Back-Door。可以这样讲，没有完全安全的操作系统。但是，可以对现有的操作平台进行安全配置、对操作和访问权限进行严格控制，提高系统的安全性。因此，不但要选用尽可能可靠的操作系统和硬件平台。而且，必须加强登录过程的认证（特别是在到达服务器主机之前的认证），

确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

6.3.4 应用的安全风险分析

应用系统的安全跟具体的应用有关，它涉及很多方面。应用系统的安全是动态的、不断变化的。应用的安全性也涉及到信息的安全性，它包括很多方面。

（1）应用系统的安全是动态的、不断变化的

应用的安全涉及面很广，以目前 Internet 上应用最为广泛的 E-mail 系统来说，其解决方案有几十种，但其系统内部的编码甚至编译器导致的 BUG 是很少有人能够发现的，因此一套详尽的测试软件是相当必要的。但是应用系统是不断发展且应用类型是不断增加的，其结果是安全漏洞也是不断增加且隐藏越来越深。因此，保证应用系统的安全也是一个随着网络发展而不断完善的过程。

（2）应用的安全性涉及到信息、数据的安全性

信息的安全性涉及到机密信息泄露、未经授权的访问、破坏信息完整性、假冒、破坏系统的可用性等。由于企业局域网一般跨度不大，绝大部分重要信息都在内部传递，因此信息的机密性和完整性是可以保证的。对于有些特别重要的信息需要对内部进行保密的（比如领导子网、财务系统传递的重要信息）可以考虑在应用级进行加密，针对具体的应用直接在应用系统开发时进行加密。

6.3.5 管理的安全风险分析

管理是网络中安全最最重要的部分。责权不明、管理混乱、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。责权不明，管理混乱，使得一些员工或管理员随便让一些非本地员工甚至外来人员进入机房重地，或者员工有意无意泄露他们所知道的一些重要信息，而管理上却没有相应制度来约束。

当网络出现攻击行为或网络受到其他一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求我们必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。

建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是管理制度和管理解决方案的结合。

6.3.6 黑客攻击

黑客们的攻击行动是无时无刻不在进行的，而且会利用系统和管理上的一切可能利用的漏洞。公开服务器存在漏洞就是一个典型例证，黑客可以轻易地骗过公开服务器软件，得到 UNIX 的口令文件并将之送回。黑客侵入 UNIX 服务器后，有可能修改特权，从普通用户变为高级用户，一旦成功，黑客可以直接进入口令文件。黑客还能开发欺骗程序，将其装入 UNIX 服务器中，用以监听登录会话。当它发现有用户登录时，便开始存储一个文件，这样黑客就拥有了他人的账户和口令。这时为了防止黑客，需要设置公开服务器，使得它不离开自己的空间而进入另外的目录。另外，还应设置组特权，不允许任何使用公开

服务器的人访问 WWW 页面文件以外的东西。在企业的局域网内我们可以综合采用防火墙技术、Web 页面保护技术、入侵检测技术、安全评估技术来保护网络内的信息资源，防止黑客攻击。

6.3.7　通用网关接口（CGI）漏洞

有一类风险涉及通用网关接口（CGI）脚本。许多页面文件和指向其他页面或站点的超链接。然而有些站点用到这些超链接所指站点寻找特定信息。搜索引擎是通过 CGI 脚本执行的方式实现的。黑客可以修改这些 CGI 脚本以执行他们的非法任务。通常，这些 CGI 脚本只能在这些所指 WWW 服务器中寻找，但如果进行一些修改，他们就可以在 WWW 服务器之外进行寻找。要防止这类问题发生，应将这些 CGI 脚本设置为较低级用户特权，提高系统的抗破坏能力，提高服务器备份与恢复能力，提高站点内容的防篡改与自动修复能力。

6.3.8　恶意代码

恶意代码不限于病毒，还包括蠕虫、特洛伊木马、逻辑炸弹和其他未经同意的软件。应该加强对恶意代码的检测。

6.3.9　病毒的攻击

计算机病毒一直是计算机安全的主要威胁之一。能在 Internet 上传播的新型病毒，例如通过 E-Mail 传播的病毒，增加了这种威胁的程度。病毒的种类和传染方式也在增加，国际空间的病毒总数已达上万甚至更多。当然，查看文档、浏览图像或在 Web 上填表都不用担心病毒感染，然而，下载可执行文件和接收来历不明的 E-Mail 文件需要特别警惕，否则很容易使系统导致严重的破坏。典型的“CIH”病毒就是一可怕的例子。

6.3.10　人员的安全风险分析

FBI 和 CSI 在 2002 年对 484 家公司进行了网络安全专项调查，调查结果显示：超过 85%的安全威胁来自公司内部，有 16%来自内部未授权的存取，有 14%来自专利信息被窃取，有 12%来自内部人员的财务欺骗，而只有 5%是来自黑客的攻击；在损失金额上，由于内部人员泄密导致了 60,565,000 美元的损失，是黑客所造成损失的 16 倍，病毒所造成损失的 12 倍。这组数据充分说明了内部人员安全风险的严重危害，同时也提醒人们应加强网络内部安全建设。

内部人员造成的危害如此巨大，为什么媒体披露的却比较少呢？这是因为黑客带来的危害是比较公开的，例如篡改主页，拒绝服务攻击、网络钓鱼、编写并传播病毒等黑客行为，这些行为造成的后果影响的面比较广，因此媒体得到这些信息也比较便捷，曝光率也就比较高。相比黑客入侵，内部人员的破坏行为往往具有隐蔽性，另外有些单位怕曝光后对社会影响不好，影响单位声誉，因此不愿意向社会透露。

1. 不满的内部员工

不满的内部员工可能在 WWW 站点上开些小玩笑，甚至破坏。不论如何，他们最熟悉服务器、小程序、脚本和系统的弱点。对于已经离职的不满员工，可以通过定期改变口令和删除系统记录以减少这类风险。但还有心怀不满的在职员工，这些员工比已经离开的员

工能造成更大的损失，例如他们可以传出至关重要的信息、泄露安全重要信息、错误地进入数据库、删除数据等等。

2. 内贼和商业间谍

信息社会，信息就是价值，信息就是生产力。IT 技术的发展使得人们获取信息的速度日益加快，这也给犯罪分子提供了便利，通过一个 U 盘，几分钟的时间就可以拷走上百兆的资料，而这些资料可能价值不菲，因此说一分钟损失几千万，上亿元绝对不是危言耸听。所以，我们在安全建设上既要防止外部攻击，也要防止内部破坏和泄密。

如果内部网络的监控管理不到位，就会有许多漏洞可以被内部人员所利用以便窃取资料，目前来看，内部泄密主要是通过如下途径。

（1）将资料通过软盘、U 盘或移动硬盘从计算机中拷出带走；

（2）内部人员通过互联网将资料通过电子邮件发送到自己的邮箱；

（3）将文件打印后带出；

（4）将公用便携式计算机直接带回家中；

（5）拆卸公司计算机上的硬盘带回家中；

（6）公用便携式计算机易手后，硬盘上的资料没有处理，导致泄密；

（7）随意将文件设成共享，导致非相关人员获取资料；

（8）移动存储设备共用，导致非相关人员获取资料；

（9）将自己的笔记本带到公司，连上局域网，窃取资料；

（10）乘同事不在，开启同事计算机，浏览、复制同事计算机里的资料。

此外，还有很多其他途径可以被别有用心的内部人员利用以窃取资料。可以这样讲，对于一个没有安全管理的企业局域网来讲，就像散落在大街上的钱币一样，虽然有很多有价值的资料，但毫无安全可言。

那么如何才能解决内部人员泄密问题呢？这就要求组织配置必要的技术装备，另一方面也要加强管理，做好内部人员的保密教育，法制教育。“技术与管理”并重，才能从根本上杜绝内部人员泄密。

在技术上，目前有许多产品可以对内部人员计算机操作行为进行审计。在管理上，防范内部人员泄密要做到以下几点。

（1）建立一整套规范的安全保密制度并严格执行；

（2）要加强员工的保密教育，使他们认识到保密工作的重要意义；

（3）要有奖惩制度，对保密先进个人、单位予以嘉奖，对于泄密事故加大惩处力度，做到以儆效尤。

6.3.11 网络的攻击手段

一般认为，目前对网络的攻击手段主要表现在以下几方面。

（1）非授权访问

非授权访问是指没有预先经过同意，就使用网络或计算机资源被看作非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式：假冒，身份攻击，非法用户进入网络系统进行违法操作，合法用户以未授权方式进行操作等。

（2）信息泄露或丢失

信息泄露或丢失指敏感数据在有意或无意中被泄露出去或丢失，它通常包括，信息在传输中丢失或泄露（如“黑客”们利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账号等重要信息），信息在存储介质中丢失或泄露，通过建立隐蔽隧道等窃取敏感信息等。

（3）破坏数据完整性

破坏数据完整性是以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。

（4）拒绝服务攻击

拒绝服务攻击就是不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

（5）利用网络传播病毒

通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

6.4　安全需求与安全目标

6.4.1　安全需求分析

通过前面对企业局域网络结构、应用及安全威胁分析，可以看出其安全问题主要集中在对服务器的安全保护、防黑客和病毒、重要网段的保护以及管理安全上。因此，我们必须采取相应的安全措施杜绝安全隐患，其中应该做到：

（1）公开服务器的安全保护；

（2）防止黑客从外部攻击；

（3）入侵检测与监控；

（4）信息审计与记录；

（5）病毒防护；

（6）数据安全保护；

（7）数据备份与恢复；

（8）网络的安全管理。

针对企业局域网系统的实际情况，在系统考虑如何解决上述安全问题的设计时应满足如下要求：

（1）大幅度地提高系统的安全性（重点是可用性和可控性）；

（2）保持网络原有的特点，即对网络的协议和传输具有很好的透明性，能透明接入，无需更改网络设置；

（3）易于操作、维护，并便于自动化管理，而不增加或减少附加操作；

（4）尽量不影响原网络拓扑结构，同时便于系统及系统功能的扩展；

（5）安全保密系统具有较好的性能价格比，一次性投资，可以长期使用；

（6）安全产品具有合法性，及经过国家有关管理部门的认可或认证；

（7）分步实施。

6.4.2 网络安全策略

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。该安全策略模型包括了建立安全环境的三个重要组成部分。

（1）威严的法律

安全的基石是社会法律、法规与手段，这部分用于建立一套安全管理标准和方法，即通过建立与信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。

（2）先进的技术

先进的安全技术是信息安全的根本保障，用户对自身面临的威胁进行风险评估，决定其需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术。

（3）严格的管理

各网络使用机构、企业和单位应建立相宜的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

6.4.3 系统安全目标

基于以上的分析，我们认为局域网网络系统安全应该实现以下目标：

（1）建立一套完整可行的网络安全与网络管理策略；

（2）将内部网络、公开服务器网络和外网进行有效隔离，避免与外部网络的直接通信；

（3）建立网站各主机和服务器的安全保护措施，保证他们的系统安全；

（4）对网上服务请求内容进行控制，使非法访问在到达主机前被拒绝；

（5）加强合法用户的访问认证，同时将用户的访问权限控制在最低限度；

（6）全面监视对公开服务器的访问，及时发现和拒绝不安全的操作和黑客攻击行为；

（7）加强对各种访问的审计工作，详细记录对网络、公开服务器的访问行为，形成完整的系统日志；

（8）备份与灾难恢复——强化系统备份，实现系统快速恢复；

（9）加强网络安全管理，提高全体人员的网络安全意识和防范技术。

6.5 网络安全方案总体设计

6.5.1 安全方案设计原则

在对企业局域网网络系统安全方案设计、规划时，应遵循以下原则。

（1）综合性、整体性原则

应用系统工程的观点、方法，分析网络的安全及具体措施。安全措施主要包括行政法律手段、各种管理制度（人员审查、工作流程、维护保障制度等）以及专业措施（识别技术、存取控制、密码、低辐射、容错、防病毒、采用高安全产品等）。一个较好的安全措施往往是多种方法适当综合的应用结果。一个计算机网络，包括个人、设备、软件、数据

等。这些环节在网络中的地位和影响作用，也只有从系统综合整体的角度去看待、分析，才能取得有效、可行的措施，即计算机网络安全应遵循整体安全性原则，根据规定的安全策略制定出合理的网络安全体系结构。

（2）需求、风险、代价平衡的原则

对任一网络，绝对安全难以达到，也不一定是必要的。对一个网络进行实际研究（包括任务、性能、结构、可靠性、可维护性等），并对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定本系统的安全策略。

（3）一致性原则

一致性原则主要是指网络安全问题应与整个网络的工作周期（或生命周期）同时存在，制定的安全体系结构必须与网络的安全需求相一致。安全的网络系统设计（包括初步或详细设计）及实施计划、网络验证、验收、运行等，都要有安全的内容及措施。实际上，在网络建设的开始就考虑网络安全对策，比在网络建设好后再考虑安全措施，不但容易，且花费也小得多。

（4）易操作性原则

安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

（5）分步实施原则

由于网络系统及其应用扩展范围广阔，随着网络规模的扩大及应用的增加，网络脆弱性也会不断增加，一劳永逸地解决网络安全问题是不现实的；同时，由于实施信息安全措施需要相当的费用支出，因此分步实施，即可满足网络系统及信息安全的基本需求，亦可节省费用开支。

（6）多重保护原则

任何安全措施都不是绝对安全的，都可能被攻破。但是建立一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其他层保护仍可保护信息的安全。

（7）可评价性原则

如何预先评价一个安全设计并验证其网络的安全性，这需要通过国家有关网络信息安全测评认证机构的评估来实现。

6.5.2　安全服务、安全机制与安全技术

安全服务、安全机制与安全技术都是网络安全方案总体设计中必须考虑的，下面对它们做一个简单的介绍。

（1）安全服务

安全服务主要有控制服务、对象认证服务、可靠性服务等。

（2）安全机制

访问控制机制、认证机制等。

（3）安全技术

防火墙技术、鉴别技术、审计监控技术、病毒防治技术等。

在安全的开放环境中，用户可以使用各种安全应用。安全应用由一些安全服务来实现；而安全服务又是由各种安全机制或安全技术来实现的。应当指出，同一安全机制有时也可

以用于实现不同的安全服务。

6.6 网络安全体系结构

通过对网络的全面了解，按照安全策略的要求、风险分析的结果及整个网络的安全目标，整个网络措施应按系统体系建立。具体的安全控制系统由以下几个方面组成：物理安全、网络安全、系统安全、信息安全、应用安全、安全管理、用户安全以及安全审计。

6.6.1 物理安全

保证计算机信息系统各种设备的物理安全是整个计算机信息系统安全的前提，物理安全是保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。 它主要包括 3 个方面：

（1）环境安全

对系统所在环境的安全保护，如区域保护和灾难保护（参见国家标准 GB50173－93《电子计算机机房设计规范》、国标 GB2887－89《计算站场地技术条件》、GB9361－88《计算站场地安全要求》）。

（2）设备安全

主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

（3）媒体安全

包括媒体数据的安全及媒体本身的安全。

6.6.2 网络安全

安全系统是建立在网络系统之上的，网络结构的安全是安全系统成功建立的基础。在整个网络结构的安全方面，主要考虑网络结构、系统和路由的优化。

网络结构的建立要考虑环境、设备配置与应用情况、远程联网方式、通信量的估算、网络维护管理、网络应用与业务定位等因素。成熟的网络结构应具有开放性、标准化、可靠性、先进性和实用性，并且应该有结构化的设计，充分利用现有资源，具有运营管理的简便性，完善的安全保障体系。网络结构采用分层的体系结构，有利于维护管理，有利于更高的安全控制和业务发展。

网络结构的优化，在网络拓扑上主要考虑到冗余链路、防火墙的设置和入侵检测的实时监控等。

1．访问控制及内外网的隔离

访问控制可以通过如下几个方面来实现。

（1）制定严格的管理制度

可制定的管理制度相应有《用户授权实施细则》、《口令字及账户管理规范》和《权限管理制度》等。

（2）配备相应的安全设备

在内部网与外部网之间，设置防火墙实现内外网的隔离与访问控制是保护内部网安全

的最主要、同时也是最有效、最经济的措施之一。防火墙应设置在不同网络或网络安全域之间信息的唯一出入口。

防火墙主要的种类是包过滤型，包过滤防火墙一般利用 IP 和 TCP 包的头信息对进出被保护网络的 IP 包信息进行过滤，能根据企业的安全政策来控制（允许、拒绝、监测）出入网络的信息流，同时可实现网络地址转换（NAT）、审计与实时告警等功能。由于这种防火墙安装在被保护网络与路由器之间的通道上，因此也对被保护网络和外部网络起到隔离作用。

防火墙具有以下 5 大基本功能：

（1）过滤进、出网络的数据；

（2）管理进、出网络的访问行为；

（3）封堵某些禁止的业务；

（4）记录通过防火墙的信息内容和活动；

（5）对网络攻击的检测和告警。

2. 内部网不同网络安全域的隔离及访问控制

在这里，主要利用 VLAN 技术来实现对内部子网的物理隔离。通过在交换机上划分 VLAN 可以将整个网络划分为几个不同的广播域，实现内部一个网段与另一个网段的物理隔离。这样，就能防止影响一个网段的问题穿过整个网络传播。针对某些网络，在某些情况下，它的一些局域网的某个网段比另一个网段更受信任，或者某个网段比另一个更敏感。通过将信任网段与不信任网段划分在不同的 VLAN 段内，就可以限制局部网络安全问题对全局网络造成的影响。

3. 网络安全检测

网络系统的安全性取决于网络系统中最薄弱的环节。如何及时发现网络系统中最薄弱的环节？如何最大限度地保证网络系统的安全？最有效的方法是定期对网络系统进行安全性分析，及时发现并修正存在的弱点和漏洞。

网络安全检测工具通常是一个网络安全性评估分析软件，其功能是用实践性的方法扫描分析网络系统，检查报告系统存在的弱点和漏洞，建议补救措施和安全策略，达到增强网络安全性的目的。检测工具应具备以下功能：

（1）具备网络监控、分析和自动响应功能；

（2）找出经常发生问题的根源所在；

（3）建立必要的循环过程确保隐患时刻被纠正；

（4）控制各种网络安全危险；

（5）漏洞分析和响应 ；

（6）配置分析和响应 ；

（7）漏洞形势分析和响应 ；

（8）认证和趋势分析。

具体体现在以下方面：

（1）防火墙得到合理配置；

（2）内外 Web 站点的安全漏洞降为最低；

（3）网络体系达到强壮的耐攻击性；

（4）各种服务器操作系统，如 EMIAL 服务器、Web 服务器、应用服务器，将受黑客攻击的可能性降为最低；

（5）对网络访问做出有效响应，保护重要应用系统（如财务系统）的数据安全不受黑客攻击和内部人员误操作的侵害。

4．审计与监控

审计是记录用户使用计算机网络系统进行所有活动的过程，它是提高安全性的重要工具。它不仅能够识别谁访问了系统，还能看出系统正被怎样地使用。对于确定是否有网络攻击的情况，审计信息对于确定问题和攻击源很重要。同时，系统事件的记录能够更迅速地和系统地识别问题，并且它是后面阶段事故处理的重要依据。另外，通过对安全事件的不断收集与积累并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对发现或可能产生的破坏性行为提供有力的证据。

因此，除使用一般的网络管理软件和系统监控管理系统外，还应使用目前较为成熟的网络监控设备或实时入侵检测设备，以便对进出各级局域网的常见操作进行实时检查、监控、报警和阻断，从而防止针对网络攻击与犯罪行为。

5．网络防病毒

由于在网络环境下，计算机病毒有不可估量的威胁性和破坏力，一次计算机病毒的防范是网络安全性建设中重要的一环。

网络反病毒技术包括预防病毒、检测病毒和清除病毒三种技术。

（1）预防病毒技术

预防病毒技术通过自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有：加密可执行程序、引导区保护、系统监控与读写控制（如防病毒软件等）。

（2）检测病毒技术

检测病毒技术是通过对计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等。

（3）清除病毒技术

清除病毒技术通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。

网络反病毒技术的具体实现方法包括对网络服务器中的文件进行频繁地扫描和监测；在工作站上用防病毒芯片和对网络目录及文件设置访问权限等。

所选的防病毒软件应该构造全网统一的防病毒体系，主要面向 MAIL、Web 服务器，以及办公网段的 PC 服务器和 PC 工作站。要求实现的基本功能包括：

（1）支持对网络、服务器和工作站的实时病毒监控；

（2）能够在中心控制台向多个目标分发新版杀毒软件，并监视多个目标的病毒防治情况；

（3）支持多种平台的病毒防范；

（4）能够识别广泛的已知和未知病毒，包括宏病毒；

（5）支持对 Internet/Intranet 服务器的病毒防治，能够阻止恶意的 Java 或 ActiveX 小程序的破坏；

（6）支持对电子邮件附件的病毒防治，包括 Word、Excel 中的宏病毒；

（7）支持对压缩文件的病毒检测；

（8）支持广泛的病毒处理选项，如对染毒文件进行实时杀毒、移出、重新命名等；

（9）支持病毒隔离，当客户机试图上载一个染毒文件时，服务器可自动关闭对该工作站的连接；

（10）提供对病毒特征信息和检测引擎的定期在线更新服务；

（11）支持日志记录功能；支持多种方式的告警功能（声音、图像、电子邮件等）等。

6．网络备份系统

备份系统为一个目的而存在，即尽可能快地全盘恢复运行计算机系统所需的数据和系统信息。根据系统安全需求可选择的备份机制有：场点内高速度、大容量自动的数据存储、备份与恢复；场点外的数据存储、备份与恢复；对系统设备的备份。备份不仅在网络系统硬件故障或人为失误时起到保护作用，也在入侵者非授权访问或对网络攻击及破坏数据完整性时起到保护作用，同时亦是系统灾难恢复的前提之一。

在确定备份的指导思想和备份方案之后，就要选择安全的存储媒介和技术进行数据备份，有“冷备份”和“热备份”两种。热备份是指“在线”的备份，即下载备份的数据还在整个计算机系统和网络中，只不过传到另一个非工作的分区或是另一个非实时处理的业务系统中存放。“冷备份”是指“不在线”的备份，下载的备份存放到安全的存储媒介中，而这种存储媒介与正在运行的整个计算机系统和网络没有直接联系，在系统恢复时重新安装，有一部分原始的数据长期保存并作为查询使用。热备份的优点是投资大，但调用快，使用方便，在系统恢复中需要反复调试时更显优势。热备份的具体做法是：可以在主机系统开辟一块非工作运行空间，专门存放备份数据，即分区备份；另一种方法是，将数据备份到另一个子系统中，通过主机系统与子系统之间的传输，同样具有速度快和调用方便的特点，但投资比较昂贵。冷备份弥补了热备份的一些不足，二者优势互补，相辅相成，因为冷备份在回避风险中还具有便于保管的特殊优点。

6.6.3　系统安全

系统的安全主要是指操作系统、应用系统的安全性以及网络硬件平台的可靠性。对于操作系统的安全防范可以采取如下策略。

（1）对操作系统进行安全配置，提高系统的安全性，系统内部调用不对 Internet 公开，关键性信息不直接公开，尽可能采用安全性高的操作系统；

（2）应用系统在开发时，采用规范化的开发过程，尽可能地减少应用系统的漏洞；

（3）网络上的服务器和网络设备尽可能不采取同一家的产品；

（4）通过专业的安全工具（安全检测系统）定期对网络进行安全评估。

6.6.4　信息安全

企业局域网的信息管理是在综合平衡信息机密性和可用性这两个因素的基础上，对网内的信息及其流经设备进行归类，明确它们的安全要求，并采取适当的技术手段和管理措施，到达信息安全的目标。

信息的重要程度信赖于信息流程，由于信息流程的不同，与信息流相关的用户对象、

设备的重要性也不同，例如公司内部的信息流可以分为“总经理—部门经理”、“部门经理—职员”、“职员—职员”等方式，每种方式中涉及的信息内容、共享程度、处理过程、硬件设备都有所区别。基于信息流的分析方法，可将信息划分为关键、重要、次要和一般等多个等级，信息等级的定义及相应的安全要求可综合考虑信息价值的关键性、损失或破坏后造成影响的程度以及影响产生后的可接受程度等因素。

信息管理是局域网安全管理的核心内容，所有安全保密手段和管理措施都是围绕着信息的安全展开的，同时应意识到信息管理不仅是针对信息本身，还涉及到信息的流动环节，它是一个动态管理的概念。

6.6.5 应用安全

在应用安全上，主要考虑通信的授权，传输的加密和审计记录。这必须加强登录过程的认证（特别使在到达服务器主机之前的认证），确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。另外，在加强主机的管理上，除了上面谈的访问控制和系统漏洞检测外，还可以采用访问存取控制，对权限进行分割和管理。应用安全平台要加强资源目录管理和授权管理、传输加密、审计记录和安全管理。对应用安全，主要考虑确定不同服务的应用软件并紧密注视其 Bug；对扫描软件不断升级。

应用层安全指局域网内应用的安全性，包括局域网内应用软件和业务数据的安全，局域网内应用软件包括数据库软件、Web 服务、电子邮件系统、文件传输系统和专用业务系统等。应用层安全技术有：网关防病毒技术、应用层安全扫描、应用层安全代理、应用层加密、应用层信息过滤技术等。

6.6.6 管理安全

管理安全指管理的安全性，包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化程度极大地影响着整个网络信息系统的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色定义都可以在很大程度上降低其他层次的安全漏洞。

为了保护网络的安全性，除了在网络设计上增加安全服务功能，完善系统的安全保密措施外，安全管理规范也是网络安全所必需的。安全管理策略一方面从纯粹的管理上即安全管理规范来实现，另一方面从技术上建立高效的管理平台（包括网络管理和安全管理）。安全管理策略主要有：定义完善的安全管理模型；建立长远的并且可实施的安全策略；彻底贯彻规范的安全防范措施；建立恰当的安全评估尺度，并且进行经常性的规则审核，当然，还需要建立高效的管理平台。

1．安全管理规范

面对网络安全的脆弱性，除了在网络设计上增加安全服务功能，完善系统的安全保密措施外，还必须花大力气加强网络安全管理规范的建立，因为诸多的不安全因素恰恰反映在组织管理和人员录用等方面，而这又是计算机网络安全所必须考虑的基本问题，所以应引起各计算机网络应用部门领导的重视。

1）安全管理原则

网络信息系统的安全管理主要基于 3 个原则。

（1）多人负责原则：每一项与安全有关的活动，都必须有两人或多人在场。这些人应是系统主管领导指派的，他们忠诚可靠，能胜任此项工作；他们应该签署工作情况记录以证明安全工作已得到保障。具体的活动如下。

① 访问控制使用证件的发放与回收；

② 信息处理系统使用的媒介发放与回收；

③ 处理保密信息；

④ 硬件和软件的维护；

⑤ 系统软件的设计、实现和修改；

⑥ 重要程序和数据的删除和销毁等。

（2）任期有限原则：一般地讲，任何人最好不要长期担任与安全有关的职务，以免使他认为这个职务是专有的或永久性的。为遵循任期有限原则，工作人员应不定期地循环任职，强制实行休假制度，并规定对工作人员进行轮流培训，以使任期有限制度切实可行。

（3）职责分离原则：在信息处理系统工作的人员不要打听、了解或参与职责以外的任何与安全有关的事情，除非系统主管领导批准。出于对安全的考虑，下面每组内的两项信息处理工作应当分开。

① 计算机操作与计算机编程；

② 机密资料的接收和传送；

③ 安全管理和系统管理；

④ 应用程序和系统程序的编制；

⑤ 访问证件的管理与其他工作；

⑥ 计算机操作与信息处理系统使用媒介的保管等。

2）安全管理的实现

信息系统的安全管理部门应根据管理原则和该系统处理数据的保密性，制定相应的管理制度或采用相应的规范。具体工作是：

① 根据工作的重要程度，确定该系统的安全等级。

② 根据确定的安全等级，确定安全管理的范围。

③ 制订相应的机房出入管理制度对于安全等级要求较高的系统，要实行分区控制，限制工作人员出入与己无关的区域。出入管理可采用证件识别或安装自动识别登记系统，采用磁卡、身份卡等手段，对人员进行识别、登记管理。

④ 制订严格的操作规程。

⑤ 操作规程要根据职责分离和多人负责的原则，各负其责，不能超越自己的管辖范围。

⑥ 制订完备的系统维护制度。

⑦ 对系统进行维护时，应采取数据保护措施，如数据备份等。维护时要首先经主管部门批准，并有安全管理人员在场，故障的原因、维护内容和维护前后的情况要详细记录。

⑧ 制订应急措施，要制定系统在紧急情况下，如何尽快恢复的应急措施，使损失减至最小。建立人员雇用和解聘制度，对工作调动和离职人员要及时调整相应的授权。

2．网络管理

管理员可以在管理机器上对整个内部网络上的网络设备、安全设备、网络上的防病毒软件、入侵检测探测器进行综合管理，同时利用安全分析软件可以从不同角度对所有的设

备、服务器、工作站进行安全扫描，分析它们的安全漏洞，并采取相应的措施。

3．安全管理

安全管理是指对可能造成安全威胁的各种情况进行自动或者手动管理，有效控制安全风险，达到安全管理的目的。具体内容主要包括：

（1）对安全设备的管理；

（2）监视网络危险情况，对危险进行隔离，并把危险控制在最小范围内；

（3）身份认证，权限设置；

（4）对资源的存取权限的管理；

（5）对资源或用户动态的或静态的审计；

（6）对违规事件，自动生成报警或生成事件消息；

（7）口令管理（如操作员的口令鉴权），对无权操作人员进行控制；

（8）密钥管理，对于与密钥相关的服务器，应对其设置密钥生命期、密钥备份等管理功能；

（9）冗余备份，为增加网络的安全系数，对于关键的服务器应冗余备份。

安全管理应该从管理制度和管理平台技术两个方面来实现。安全管理产品尽可能地支持统一的中心控制平台。

6.6.7　用户安全

局域网中的硬件设备、操作系统和应用系统等面向的用户主要分为管理者和使用者两大类，各种权限的设置成为用户管理的主要内容。若从可信度的角度去观察用户管理，则可以看到，用户及权限的设置正是用户可信程度高低的体现，用户所拥有的管理或使用权限越高，则其被信任的程度也越高，反之亦然。用户可信度在用户管理中是有层次关系的，用户可信度越高则所处的可信层次越高。

在通常的用户管理概念中，一个用户能够同时被赋予多种角色，行使多种权力，且这种授权方式在实现上一般仅有管理约束而无技术约束，由此产生的后果则是破坏了用户可信度的层次关系，给安全管理带来了隐患。以用户可信度为基础，用户管理首要考虑的问题就是如何有效地保证用户可信度的层次关系不被破坏。例如，一个用户只能处于一个可信层次中；由可信管理机制统一对用户实施可信度管理；用户在可信管理机制下完成其在可信层次中有条件的转换等。

局域网用户管理是合理、有效、安全地使用局域网内设备及信息系统的基础，实施用户管理除了从行政（或业务）管理角度考虑外，应更多地发挥技术管理机制作用，尽量避免因主观因素和管理疏忽带来的安全问题。

6.6.8　安全审计

安全审计的范畴涵盖安全方针、安全组织、资产分类与控制、人员安全、物理和环境安全、通信和操作管理、访问控制、系统开发与维护等内容，此处所说的安全审计则特指在网络及信息系统中对安全事件进行收集、检测、统计、分析、评估和控制的过程。

安全审计信息的来源主要为各种日志记录，如运行日志、告警日志、安全认证日志、操作日志等。安全审计信息可按照用户、时间、地址、数据、程序、设备、告警级别等分

类标准进行统计、分析。安全审计的评估过程是在对已发现的安全事件进行统计、分析的基础上，确定已经或可能造成的影响程度，并提出解决方案。安全审计的控制过程则是通过采取规范、法律、监察、管理、技术等措施达到减小安全事件影响后果的目的。

安全系统的建设不是各种安全产品的堆砌，也不是一次性安全策略配置就能完成的，而是一项长期性且需要不断完善的工作，安全审计正是这项长期工作的主要内容，是内网安全系统发挥作用的有效保证。

6.7　网络安全技术

国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此可以将计算机网络的安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可靠性、完整性和保密性。可见，解决网络安全问题是离不开网络安全技术的，那么主要的网络安全技术都包括哪些呢？这里我们对主要的内部网络安全技术做一个简单的介绍。

6.7.1　桌面管理

随着信息技术的发展，企业内部越来越多的人员通过个人计算机来完成日常办公，个人计算机已经成为企业 IT 资产中最大的一个组成部分。

由于个人电脑的数量庞大，使用人员复杂，位置分散，因此对企业的信息安全带来了巨大的挑战，例如如何及时统计大量的 PC 的软、硬件配置情况，如何了解众多 PC 的安全状态，如何对 PC 存在的安全问题（例如安全漏洞）快速响应，如何防止个人在 PC 上进行违反组织安全策略的行为，如何防止机密信息通过 PC 流失等等。

针对上述安全挑战，提出了桌面安全管理系统。桌面安全管理系统是一个企业级的终端安全管理解决方案，通过使用该产品，企业可以有效地对数量众多的桌面管理进行安全防护和控制，从而贯彻有组织的安全策略，实现端到端的安全管理。

1．系统结构

桌面安全管理由管理中心服务器和桌面安全代理组成，服务器实现对终端的集中管理和控制，桌面安全代理则被安装到每一台被管理的终端，执行各种安全防护和管理任务。

服务器部署根据企业情况不同又可以分为一级（集中）部署，或者分级部署。

所谓一级（集中）部署，即在企业集中部署一台服务器，包含各种组件，管理企业所有终端的情况，这种情况适用于终端数量少，分布范围小的情况。

所谓分级部署，即在企业按照机构分布或者地理位置进行分级部署，在分支节点部署二级管理组件，这种适合更大规模的终端的管理。

2．系统功能

桌面安全管理系统针对终端管理的安全需求，提供了丰富而强大的功能，系统主要功能包括：

（1）资产管理

支持基于逻辑组的资产管理机制，能够自动根据操作系统、用户所在部门等进行资产

分组。可查看每个资产的实时在线情况、软件硬件配置、安全评估、告警日志、漏洞报告等信息。另外还提供资产树结构方便使用。

（2）终端用户管理

系统支持使用者的人力资源信息和资产硬件相绑定的功能，资产和用户的绑定能够帮助管理员快速地定位责任人，处理安全违规事件。系统还提供每个人的绑定资产历史记录情况。

（3）终端用户自服务系统

普通用户可以使用姓名、工号和密码登录进入自服务系统，提交终端维护工单、扫描自己的漏洞、下载补丁、查看最新安全文摘等。

（4）多角色权限控制

提供管理员、审计员、组管理员、终端用户等角色，管理员可以方便地控制角色和具体的人员的权限。

（5）配置变更管理

系统不仅支持最新的终端配置变化情况，还提供每个配置变更情况的历史记录功能，用户可以查询某个 IP 地址的使用情况。

（6）安全评估

系统不仅提供每个资产、每个组织结构的实时安全评估，而且提供整个可以管理的网络的实时安全评估以及趋势图。这样系统管理员可以直观地了解目前整个网络的安全状况。

（7）漏洞扫描

系统提供专业的基于主机的漏洞扫描功能，扫描结果自动汇总为漏洞报告，通过补丁漏洞库为用户提供专业的漏洞防护。不仅可以扫描 Hotfix 升级类型漏洞，还可以扫描系统的潜在配置性的漏洞，例如弱口令。

（8）补丁分发

系统支持自动根据漏洞扫描的结果进行补丁下发，支持定制补丁下发参数，支持根据补丁特性自动过滤不同操作系统的补丁。

（9）远程控制

系统支持实时的远程控制，操作对方的桌面犹如自己的桌面一样，提供管理员远程技术支持的能力。

（10）软件分发

系统支持实时的软件分发功能，管理员只需将需要分发的软件上传到服务器，可以同时分发软件给一个组的终端、或者多个组的终端上。

（11）软件监控

系统支持软件黑白名单的功能，例如必须安装杀毒软件，不能安装游戏软件等。

（12）非法外联监控

系统支持对终端的拨号行为的控制，可以实时截断终端的拨号行为并且发送告警。监控策略可以设置监控时间、监控拨号的号码段等。

（13）屏幕监控

系统不仅支持实时的截取对方的屏幕图像，而且支持定期的按照既定策略截取屏幕。

管理员将很方便地获得对方的违规依据。

（14）USB 存储设备监控

系统支持基于策略的 USB 存储设备监控，这些设备包括 U 盘、移动硬盘等。当终端用户违规使用这些设备的时候，将可能被记录并且被禁止使用。

（15）强大的安全审计功能

提供 QQ/MSN 聊天记录审计，文件使用（复制，移动、删除、打开）记录审计，窗口打开记录审计、键盘记录审计、I/O 设备使用审计、网络访问审计等审计模块供选择。

（16）强制安全策略

系统支持为每个资产或者用户定义强制安全策略，强制安全策略本身包含了其他各种不同的安全策略，例如补丁、非修补类型的漏洞、软件安装、拨号、USB 设备的使用等等一系列的策略。当用户违反强制安全策略，将执行响应动作，包括 EMAIL 告警通知管理员或者直接关闭终端的网络连接。

（17）终端接入控制

有效控制终端接入网络，用户的终端必须通过用户身份认证、设备安全检查等安全控制手段后，才能接入内部网络，防止非法用户或存在安全隐患的终端，对网络带来危害。

3．系统特点

桌面安全管理系统是一个复杂的系统，是网络安全体系建设中的一个重要组成部分，一个完整的、功能强大的桌面安全管理系统应该具有以下特点：

（1）全面的终端安全管理

对终端进行全面的安全管理，包括资产、软硬件配置、漏洞、补丁、监控、接入等各个方面。

（2）强大的漏洞补丁管理

系统能够根据终端和漏洞的情况，自动匹配最合适的安全补丁，并自动下发到终端。使用补丁漏洞库可以轻松地管理漏洞和补丁信息。

（3）强制安全策略

绑定到终端用户的强制安全策略，使得不论用户实际使用的资产如何变化，都能一致地执行安全策略。

（4）细致的安全监控和审计

系统提供全面的安全监控和审计功能，能够对多种用户行为进行监视，有效防止关键信息的非法外泄。

（5）系统安全级别评估

系统不但能够对各个安全细节进行管理，更能够提供整体的安全评估，帮助管理员从微观到宏观，均能把握网络的安全状态。

（6）终端和人员的关联

能够快速收集资产和责任用户的关联关系，极大提高管理员的工作效率，轻松实现代理的分发。

（7）稳定可靠

桌面管理系统要求设计合理，并严格测试，具有良好的稳定性；系统提供自备份和自恢复功能，保证可靠运行。

6.7.2 网络管理

随着国内外对网络应用需求的迅猛增长，网络环境也变得越来越错综复杂，如何高效、可靠地利用这些网络资源，逐渐成为众多的企事业单位所关注的问题。

网络管理系统是为了从根本上解决网络管理难（如：利用率不高、排除故障难等）的难题而开发。网络管理系统主要包含网络五大管理功能（五大管理功能是指性能管理、配置管理、安全管理、故障管理和计费管理）中的配置管理、性能管理和故障管理，同时也实现了部分安全管理的功能，实现了自动拓扑发现、实时的性能管理和及时解决的故障管理。网络管理系统能有效帮助网络管理人员提高网络利用率和网络服务的质量。

1．管理对象及内容

（1）路由器、交换机等大部分常用网络设备，网络设备根据具体网络环境而有所不同，具体包括以下内容：

① 对网络设备的 CPU 实时监视；

② 对设备各个端口的监视（up，down，administrative down）；

③ 网络设备的自动发现；

④ 对设备端口所连的链路进行监视（有没有延时，有没有丢包）；

⑤ 对网络设备路由信息的实时监视；

⑥ 网络设备的资源管理。

（2）网络链路，对于一个有一定规模的网络，其中会存在大量的网络链路，对这些链路上的信息进行监视有利于及时发现网络运行状况。

① 对网络链路的实时监视（如流量、负载等）；

② 对网络链路的监视（up，down，administrative down）；

③ 网络链路的类型；

④ 网络链路的自动发现；

⑤ 网络链路的延时测试。

（3）服务器

网管系统应该能对不同平台（Windows，UNIX， Linux），不同应用（WWW，FTP，Telnet）的服务器进行实时监视。包括：

① CPU 的监视；

② 各种服务的监视；

③ 服务器的资源管理和进程管理；

④ 安全管理。

（4）PC

PC 是网络中的一个重要组成部分，对其运行状态进行管理自然也成为网络管理系统的功能之一了，具体项目包括：

① 对主机管理包括 Web 管理，Telnet 管理等常用网络工具；

② 对主机设备实时状态信息的监视；

③ PC 的资源管理和进程管理；

④ 安全管理。

（5）外设

除了 PC 以外，还需要对 PC 的外设进行一定的管理，以便出现故障时能够及时找到安全问题。

① 资源管理；

② 维护管理。

网络管理系统通过对以上基本网络组成元素的监视与监控，模拟真实的网络环境，为用户提供了统一的操作和查看界面，方便用户通过网络管理系统实时地了解整个网络的运行情况和状态。同时，系统提供了多方面的主动监视异常情况，并主动通过提示框、邮件、短信等方式通知用户。

2．系统结构

网络管理系统采用先进且成熟的 MVC 模式，三层架构，显示层、逻辑层和业务逻辑层完全分离，显示界面可以十分方便地更换。同时，后台服务和应用程序也可以完全分离，便于系统的维护和调试。数据库访问使用一个访问层加以封装，用户可以方便地更换数据库。

整个网络管理系统采用先进、灵活的分布式架构：数据库、应用程序和服务 3 个部分可以分布在任意的 3 台计算机上。系统默认的分布是配置在同一台计算机上的。

3．系统特点

网络管理是一件复杂而繁琐的工作，要通过网络管理系统来有效地解决这个问题的话，必然对网络管理系统提出较高的要求。

（1）系统简单、易用性

网络管理系统以简单、易用、实用和适用作为第一追求方向，主要体现在如下几个方面：

① 采用友好、易于理解的全中文界面、中文注释，常用功能按钮化，简化使用；

② 界面风格用户定制（Windows 风格，UNIX 风格等），操作简便；

③ 回避复杂晦涩的专业网络术语，以直观易懂的方式，对重要的网络术语进行用户能理解的诠释。

④ 对于网络参数进行再加工，让系统管理人员完全理解“数据”传达的信息；同时根据用户的需求定制各种数据加工功能。

（2）系统功能全面性

网络管理系统的功能全面性主要体现在：

① 全面提供了网络管理人员在网络管理中所使用的的全部功能，但对一些极少用，而又不重要的功能坚决摒弃；

② 基于多种操作系统，多种网络平台。

（3）系统安全、可靠性

采用应用与服务分离的 MVC 软件架构。在日常使用中，可以在多个备份的主机上开启服务，当主要的管理主机出现故障时，可以在备份主机上开启业务，对网络进行管理。

采用集中式的网络管理模式，并且对用户的权限进行严格的划分和认证。

（4）系统极强的适应性和通用性

网络管理系统可以对市场上现有的大多数主流厂商的网络设备进行管理，包括 Cisco，3Com，Bay，Juniper，Extreme，Foundry，Nortel，华为，港湾，中兴，博达，实达，迈普等厂商设备。系统可以对支持 SNMP 的网络设备实施统一的管理，对不同的主机系统实施服务管理。针对国内用户的网络管理实际需求，网络管理系统提供大量实用功能，让用户同时做到了“最合理的配置”与“最好的管理”。

（5）系统良好的可拓展性和定制性

网络管理系统全中文的自主开发，利用先进的组件思想，标准的建模语言，为后续二次开发打下了坚实的基础。可以根据用户的需求，灵活地进行各种扩充。

（6）系统具有很好的个性化特性

提供了系统界面配置功能。网络管理员可以根据个人喜好对系统的显示进行定制，包括拓扑显示，故障提示等。

（7）系统特有的决策支持、分析型特性

利用先进的统计模型，对采集到的数据进行统计分析，形成了丰富的决策支持、分析报表。同时，为了满足特定用户对特定分析的要求，公司提供高效、优质的“二次开发”服务。

（8）系统的主动性明显地优于其他系统

系统充分考虑到让用户去找问题的烦琐和工作量，因此，网络管理系统充分地提供了系统自动监测和报警功能，系统主动监测到各种异常情况，并按用户设定的方式提示用户，极大地方便了用户对网络的故障和性能管理。

（9）优异的性价比

在衡量一个系统是否适合自己时，系统自身的性价比是一个非常重要的因素，只有做到物有所值，甚至物超所值才是我们所追求的。

4．完善的系统功能

网络管理系统包括如下常用的网络管理功能：拓扑图、编辑与查看、性能分析、资源管理、事件与告警、工具、系统管理、日志、帮助

（1）拓扑图管理

网络管理系统的拓扑发现和拓扑图的显示是同时进行的，拓扑图实现了分层显示，顶层是三层拓扑发现的结果，显示的是三层设备和子网以及它们之间的连接视图。具体包括以下特点：

① 系统能够自动生成三层网络拓扑图和子网的物理视图，并且支持手动的设备拓扑伸展；

② 系统支持用户手工添加网络设备至拓扑图；

③ 系统能够界面化显示设备和链路状态；

④ 系统支持实时编辑显示规则和对图片的导出；

⑤ 系统支持实时采集设备和链路状态信息，动态更新网络拓扑图。

⑥ 支持逼真地显示 Cisco，3Com，Bay，Juniper，Extreme，Foundry，Nortel，华为，港湾，中兴，博达，实达，迈普等各主流厂商网络设备的背板图；

⑦ 用户可直接在逼真的各设备背板图上选择查看各模块和端口的各类网络和连接设

备的信息。

（2）编辑与查看管理

查看网络设备信息是网络管理员经常使用的功能，网络管理系统的信息查看分为以下几个方面：

① 系统能够查找和替换拓扑中的设备；

② 系统能够对设备名称进行个性化编辑；

③ 系统能够查看服务器实时信息；

④ 系统能够查看链路实时信息；

⑤ 系统能够查看端口实时信息；

⑥ 系统能够查看设备真实视图。

通过该菜单项，管理员能查看拓扑图中设备、端口和链路的实时状态信息，能够查看设备的真实背板图，并且，通过背板图能对设备的端口进行管理。

（3）性能分析管理

网络管理系统提供基于设备和基于端口的性能分析，用户可以以小时为单位、每次轮询（更细致）或自定义时间间隔为单位显示指定设备（路由器、交换机或服务器等设备）的性能图表，并能以三维立体或折线形式表现出来。网络管理系统同时提供了端口的实时性能分析，供用户对某个端口实时监控并能分析一段时间内的实时记录。

① 系统支持基于周期轮询的系统性能指标的统计；

② 系统支持自动生成各种报表（含日报、周报、月报和自定义时间段报表）；

③ 系统支持性能统计结果的 3 种图形显示（曲线、柱状图和饼状图）；

④ 系统支持基于设备端口的实时性能分析；

⑤ 系统支持对实时分析记录的保存和读取。

网络实时性能分析对网络运行情况进行了实时、详细的表现。

（4）资源管理

资源管理用于查看网络上的硬件和软件资源，以及定位和管理 IP 资源。在设备资源发生变化时，能及时刷新显示，用户也可以根据自己的网络规划，对软硬件资源和 IP 资源进行合理的管理。

① 系统按设备种类（路由器、交换机、服务器、PC、外设等）建立主机上硬件资源的管理和监控，并以颜色区分设备信息的状态（内存快照或保存到数据库）；

② 可以方便地把主机设备设置为服务器，也可将服务器设置为主机；

③ 对设备的操作支持批处理和编辑维护记录；

④ 系统提供自定义静态和动态 IP 范围，以方便对 IP 资源的管理；

⑤ 以棋盘状的布局显示 IP 分布图，并且可以记录下多次 IP 分布的状况。

（5）事件与告警管理

网络规模的扩大对网络的“实时性能”和“可靠性”的要求特别高。网络管理系统特别地加强了对这方面的实时监控。通过对这些信息的监视，可及时了解网络运行的瓶颈，以及用户对本地 IP 的使用情况，而且提供了 6 种快捷、有效的告警方法，在第一时间，以用户设定的方式通知网络管理员“网络的异常情况”。

① 实现查看网络设备（交换机和三层交换机）端口逻辑上直连的 mac 地址及相关信息；

② 以 IP-MAC 绑定形式实现对设备的网络连接权限控制（分时段或分网段），并可批量处理；

③ 系统支持基于端口、设备、链路和服务状态的监视；

④ 系统支持告警事件和告警规则设置；

⑤ 系统自动告警功能：声音、程序、E-mail、消息框、列表框和手机短信五种告警方式。

（6）网络工具管理

网络管理系统集成了常用的网络诊断工具，使管理员不需要脱离本系统的操作界面，就能对一些常见的网络故障进行诊断和排除，真正做到了方便、快捷。

① 系统支持 telnet 管理；

② 系统支持 ping 工具；

③ 系统支持 traceroute 工具；

④ 系统支持 Web 方式管理；

⑤ 系统支持链路时延测试；

⑥ 系统支持主机定位工具；

⑦ 系统支持路由信息工具。

（7）系统管理

系统管理对网络管理系统提供了完善的管理体系，对不同用户可以赋予不同登录权限，提高软件的安全性和可靠性。当管理员暂时离开时，可以将界面锁定，禁止他人使用该系统。执勤人员的排定，数据库的备份恢复，以及 SNMP 规则设置，网络管理员可以通过选项配置管理，按照自己的习惯，配置相关的 SNMP 全局信息和局部子节点信息。

① 系统支持多用户管理（添加用户及权限分配）；

② 系统支持执勤人员设置；

③ 系统支持界面锁定功能；

④ 系统支持数据库的备份和恢复；

⑤ 系统支持 SNMP 设置。

（8）日志管理

日志管理是保证系统安全可靠不可缺少的一部分，系统提供了 3 种不同的日志备份，而且，用户可以组合查询符合条件的日志。

① 系统日志备份管理；

② 系统操作日志管理；

③ 系统事件日志管理；

④ 系统告警日志管理；

（9）设备背板图

在充分了解“用户需求”的基础上，在网络管理系统中提供常用设备的真实专用背板图和通用背板图，支持各种主流厂商设备的真实背板显示和相关操作。同时，考虑到用户对有些背板图的特殊性要求，因此，也提供为用户定制的服务。

我们提供的背板图与真实网络设备一一对应的，管理员能方便有效地对网络设备端口进行监控和管理。

（10）帮助管理

帮助管理是帮助用户高效、友好地使用网络管理系统的重要组成部分。用户通过帮助栏不仅可以方便地获取版权、软件配置、系统配置和图标说明等信息，还可以查看用户手册和一些常见异常问题的解答。

6.7.3　网络监控审计

局域网面临的安全问题包括网络系统安全和数据安全。在网络系统安全方面，需要防止网络系统遭到没有授权的存取或破坏以及非法入侵；在数据安全方面，需要防止机要、敏感数据被窃取或非法复制、使用等。网络安全监控审计系统可以对局域网中的计算机用户的行为进行监控、审计，防止内部机密信息的泄露，并能帮助高层管理人员监督员工合理高效地使用计算机。

网络安全监控审计系统主要实现以下目标：对内网用户进行安全监视和行为审计；从网络通信和外接设备等方面进行信息传输复制限制；管理系统资源防止受到攻击；加固系统，分发补丁。

1．系统结构

网络安全监控审计系统由 3 部分组成，即客户端、控制台和服务器端。客户端安装在每一台需要被监视的计算机上，用来收集数据信息，并执行来自服务器模块的指令。服务器端一般安装在一台具有高性能 CPU 和大容量内存的用作服务器的计算机上，用来存储和管理所有安装有代理模块的计算机的数据。控制台一般安装在公司的管理人员的计算机上，用来监控每台安装有代理模块的计算机，管理各类审计系统，制定安全策略。

2．系统主要作用

（1）事先预防

1）设备使用监控

可禁止各种类型的设备，包括软驱、光驱（包括刻录机）、磁带驱动器、USB 存储设备、串/并口、SCSI、IEEE1394 总线、调制解调器、红外通信设备、USB，以及笔记本电脑使用的 PCMCIA 卡接口。

2）应用程序监控

可以禁止运行指定的应用程序，或者只允许运行指定的应用程序。

3）上网行为监控

可以禁止访问指定的网站，或者只允许访问指定的网站。

4）文件操作监控

可限制对指定文档的访问，限制指定的计算机或组的用户对文档进行的操作，包括访问、创建、复制、移动、改名、删除、恢复以及文档打印等操作。

5）网络访问监控

可指定禁止非法外连，禁止未安装客户端代理模块的计算机接入网络，与安装了客户端代理的计算机进行通信。

（2）事中监控

① 报警响应

根据设备使用规则、应用程序规则、上网行为规则、文件操作规则、网络访问规则等

进行监视，对违反规则的行为进行报警。根据事先规定的响应策略进行响应，尽可能阻止事态扩大。

② 终端屏幕监视

可根据需要进行终端屏幕监视，随时掌握终端用户的使用情况。

（3）事后审计

① 历史数据备份

收集代理模块采集的数据，并将其保存到数据库中。

② 数据查询统计

可查询特定机器特定时刻的历史记录；查看监测日志、系统日志和管理员的操作日志并进行分析和审计。

（4）其他功能

① 用户及权限管理

包括添加、删除、修改管理员，系统管理员采用分权分级的管理方式，每个管理员都有其授权工作范围和管理权限。

② 规则管理

包括时间段、网站组、应用程序组、硬件设备接口、应用软件等，可进行归类，便于规则的设定。

③ 报表设置

可以对文件监视、应用程序监视、网站监视、系统事件、应用程序统计、网站访问统计、日志查询等报表格式进行设定。

④ 软件分发

根据漏洞扫描系统扫描的结果，将需要安装的系统补丁分发到各个客户机终端上。也可以根据用户需要，分发其他的软件程序到客户机终端上。

3．系统特点

（1）全面防止重要信息外泄

① 禁止使用非授权的存储设备（如：软盘、移动硬盘、刻录机等）；

② 禁止使用任何的通信端口（如：USB、串口、红外线等）；

③ 禁止使用打印机设备；

④ 详细记录终端 PC 文件的使用操作；

⑤ 禁止非授权的网络访问。

严格控制信息输出渠道，对计算机的各种设备进行管理，包括存储设备（软驱、光驱、刻录机、磁带驱动器、USB 存储设备）、通信设备（串口、并口、调制解调器、USB、SCSI、1394 总线、红外通信设备以及笔记本电脑使用的 PCMCIA 卡接口）及文件打印控制，使信息流向达到控制，保证信息不被随意外泄。

与此同时，还详细记录终端 PC 用户对文件的各种操作，包括对文件的创建、打印、访问、复制、改名、恢复、删除、移动等，方便事后查阅。管理者还可以选择记录终端 PC 的屏幕快照，根据需要播放操作记录。

网络安全监控审计系统从事前预防（对各种设备的控制），事中监控（屏幕快照），事后审计（屏幕快照回放，操作记录查询等），全面防止重要信息外泄。

（2）进行 IT 资产管理

① 自动获取终端 PC 硬件配置信息；

② 自动获取终端 PC 所安装的软件信息；

③ 自动获取和控制终端 PC 当前运行的系统进程；

④ 自动获取和控制终端 PC 当前的共享目录；

⑤ 查询终端 PC 的 IP/MAC 地址；

⑥ 查询终端 PC 的系统启动项目信息。

网络安全监控审计系统可以对终端 PC 的硬件、软件信息，控制终端 PC 的共享及运行的程序，管理员可终止终端 PC 运行的非法程序，关闭其共享的文件夹（包括 Windows 的默认共享）。

（3）有效监控网络资源使用

① 禁止非授权的计算机访问网站；

② 禁止授权计算机访问非授权的网站；

③ 实时监视并记录各计算机访问的网站信息；

④ 实时监视对各计算机特定端口的访问连接；

⑤ 对非法接入的设备（如：笔记本电脑）进行完全隔离，使其无法对系统资源有任何的操作权限；

⑥ 防止对非授权资源的操作；

⑦ 对特定文件的访问进行控制，禁止非授权的操作（如：读取、复制、删除等）对特定文件的访问进行实时监视，实时报警；

⑧ 禁止对系统关键配置信息进行查看、更改（如：更改 IP/MAC 地址、使用设备资源管理器等）；

⑨ 禁止终端 PC 通过非法拨号方式接入 INTERNET；

⑩ 禁止运行特定的应用程序（如：QQ、MSN 等聊天工具）并提供实时性报警。

网络安全监控审计系统记录员工常用的网络活动，通过封堵 QQ，MSN 等聊天工具、网络游戏、股票等程序，限制上网站点规范员工的网络行为，使网络资源得到有效利用。

（4）审计系统信息和用户操作行为

① 详细记录管理员对系统进行的所有配置操作；

② 详细记录终端 PC 文件的使用操作（如：复制、删除、移动、打印、更改等）；

③ 针对终端 PC 使用应用程序的情况进行详细的记录；

④ 对于终端 PC 使用的应用程序和浏览网站的信息进行统计并能以列表、柱形图和饼图等样式显示结果；

⑤ 轻松对多种操作信息提供快速查询功能（如：文档监视、应用程序监视、系统信息等）；

⑥ 多种重要的审计信息可以生成个性化的报表；

⑦ 对终端 PC 的各种操作以屏幕快照的方式记录，查询方便。

网络安全监控审计系统可记录管理员的操作，只有审计员才能删除相关记录，这样可对管理员的权利进行制约，防止因管理员权限过大而形成安全隐患。对终端用户的行为进行记录和审计可帮助进行事后追查，能对用户行为进行更多了解。

（5）安全、卓越的系统性能

① 管理权限分级，利于分级控制；

② 服务器端与客户端之间应用了严格的身份认证，防止未授权使用，保障系统的管理安全；

③ 客户端、服务器及控制台间的数据传输全部采用加密传输方式，防止传输的数据被窃听；

④ 备份和恢复服务器数据库中的信息，保证历史记录的方便查阅；

⑤ 在终端 PC 上运行的客户端软件采用了透明模式，用户察觉不到本地已安装客户端软件；

⑥ 客户端软件采集数据信息不影响终端 PC 的使用性能；

⑦ 传输中的数据经过特殊压缩，对网络带宽的占用非常少；

⑧ 对非法接入的主机可切断其与内部安装过客户端代理主机之间的联系；

⑨ 本地用户不能自行卸载、关闭客户端代理程序。

（6）灵活的自定义规则

① 可以制定不同的周期规则，以保证工作时间、节假日等时间应用不同的规则；

② 可以自定义各种应用程序的访问或禁止；

③ 可以针对不同的个人、用户组，来制定不同的规则策略。

网络安全监控审计系统提供的自定义规则非常灵活。管理者可以定义不同的时间（如，上班时间，下班时间，公休日）有不同的规则，也可以对不同的用户组或者终端 PC（如，管理层，普通职员）定义不同的策略，以保证网络的资源合理分配。

4．系统部署

网络安全监控审计系统的部署非常简单。一般将客户端安装到需要保护或监控的终端 PC/服务器上，将服务器端安装在一台 PC 或服务器上，而控制台可以放在公司的任何位置，安装在相关的主管人员的计算机上，即可对网络进行监控。

在各种部署安装完成之后，一般根据实际需要，采取如下措施：

（1）对所有计算机，都禁止使用拨号进行非法外连，防止出现安全隐患；

（2）对所有计算机，都禁止非法主机接入，保证整个网络都与外界严格隔离，又不影响正常使用；

（3）对所有计算机，都禁止访问除内部网站外的其他网站；

（4）对所有计算机，都禁止运行聊天和游戏软件；

（5）对所有计算机，都禁止修改网络属性，包括 IP 地址等；

（6）对所有计算机，都强制关闭了系统的默认共享，防止出现漏洞；

（7）对大部分计算机都禁用了通信设备、输出设备和外接存储设备，保证从这些计算机无法将网络中的数据复制或打印；

（8）对所有计算机，设置补丁分发规则，定时升级；

（9）对试图违反以及试图改变以上安全策略的行为都进行报警和采取锁定计算机的响应策略；

（10）由主管领导亲自掌握设置屏幕监视的权限，对指定的计算机进行屏幕监视；

（11）定期汇总统计文件操作记录、应用程序记录、网站访问记录、硬件设备记录和

报警记录，检查是否有违反安全策略的行为。

6.8　网络安全服务

计算机网络是一个不断发展和完善的过程，同样网络安全也是动态变化的，特别是新技术和新应用的出现，使用任何一种“静态”或者号称“动态”防范的产品都不能解决一直在发展的网络安全问题，因为在现实环境中：

（1）安全是动态的不断变化和发展的过程，单纯的产品部署无法确保整体安全；

（2）安全建设是一项复杂的系统工程，安全不是简单的产品的累加；

（3）安全产品无法解决所有问题；

（4）人员的操作水平和系统的复杂性之间的差距，造成现有的系统管理员对目前先进、复杂的网络的管理能力有限。

网络安全绝不是安装几个流行的网络安全产品就能解决问题的，它需要合适的安全体系和合理的安全产品组合，需要根据网络及网络用户的情况和需求规划、设计和实施一定的安全策略以及其他多种安全服务。

安全服务与安全产品是相辅相成的，一方面，脱离服务的产品无法发挥其固有的功能，另一方面，脱离产品的服务只能是纸上谈兵、空中楼阁。

安全服务的重要意义在于以下几个方面：

（1）如何使安全产品发挥应有的作用，以及如何评价和验证安全产品的有效性？

（2）安全产品、安全服务、安全管理以及人员教育都是安全体系建设中不可缺一的部分。

（3）安全产品解决不了所有的安全问题。

对安全事件的处理不能只靠事后处理（应急响应），而应该通过系统的网络安全服务建立起完整的网络信息安全体系，做到预先防御和保障。

6.8.1　借用安全评估服务帮助我们了解自身安全性

为了系统全面地了解计算机网络系统的安全性，需要通过安全评估来实现，安全检查的评估项目包括如下内容：

（1）网络基础环境与结构；

（2）网络应用系统；

① 服务器，工作站

② 网络设备

③ 应用服务

④ 数据库

（3）信息资产的分类与控制；

（4）数据通信与存储状况；

（5）组织在信息安全方面的政策与制度；

（6）安全策略实施与应用状况。

对网络应用系统的评估可以采用现场评估和远程评估两种方式提供分析报告，评估内

容包括以下几个方面。

1．主机安全评估（UNIX 平台）

（1）系统类型

- SunOS 5.5-8
- Solaris2.5-8
- Linux
- *BSD

（2）用户安全

- 控制台安全
- 用户口令安全
- 用户文件及目录许可权限安全
- 其他

（3）操作系统安全

- 系统日志/审计策略
- 受信主机安全
- 安全终端设置
- 系统文件完整性及存取许可安全
- SUID/SGID 许可程序安全
- 其他

（4）网络服务安全

- HTTP 服务安全
- DNS 服务安全
- 网络文件系统 NFS 安全
- Telnet 服务安全
- FTP 服务安全
- SMTP 服务安全
- POP 服务安全
- Finger 服务安全
- X window 系统安全
- RPC 服务安全
- 其他网络服务安全

（5）系统程序安全

- 危险程序访问权限
- 后门程序检测
- 提供评估报告

2．主机安全评估（Windows 平台）

（1）系统版本

- Windows NT
- Windows 2000

- Windows XP
- Windows 2003

（2）用户安全

- 口令安全管理
- 账户锁定设置选项
- 来宾账号安全管理
- 其他

（3）操作系统安全

- 文件系统安全特性
- 设置审计策略
- 进行组管理
- 信任域的管理（主要基于 LAN）
- 其他

（4）网络服务安全

- HTTP 服务安全
- DNS 服务安全
- Telnet 服务安全
- FTP 服务安全
- SMTP 服务安全
- POP 服务安全
- Windows 服务安全
- 共享服务安全
- Proxy 服务安全
- 其他网络服务安全

（5）系统程序安全

- 危险程序访问权限
- 后门程序检测

3. 主机安全扫描

采用专用主机安全扫描设备对主机的安全状况进行分析和检测。

4. 互联网应用评估

- Web Servers
- CGI 程序安全
- 其他

5. 数据库安全评估

- 数据库(SQL Server)
- 数据库(Oracle，Sybase)

6. 网络安全设备评估

- 防火墙
- IDS

- 加密机
- 物理隔离
- 其他

7. 网络效率及故障检测

- 网络流量分析
- 对可疑内容的检测和分析
- 网络协议及性能的分析
- 提供分析报告

8. 渗透测试

- 在客户许可和可控的情况下，采用常用的黑客攻击手法，模拟黑客攻击
- 提供分析报告

9. 入侵检测

- 安装部署入侵检测系统，提供入侵检测报告
- 定期向管理员提供入侵检测报告

6.8.2 采用安全加固服务来增强信息系统的自身安全性

安全加固服务就是利用多种技术手段对网络信息系统中的操作系统平台和重要的网络设备提供安全加固和配置优化，安全产品只能从表面上隐蔽安全隐患，而安全加固服务则可以从本质上清除安全隐患，购买和部署安全产品从广义上讲也应归属于安全加固服务中的一个应用手段。

安全加固服务的内容包括以下内容。

（1）操作系统安全修补、加固和优化；

（2）应用服务安全修补、加固和优化；

（3）网络设备安全修补、加固和优化；

（4）现有安全制度与策略的改进和完善，具体包括以下内容：

①机房管理；②办公环境管理；③主机系统管理；④数据管理；⑤用户管理；⑥安全设备管理；⑦物理设备管理；⑧网络应用管理；⑨应用业务系统管理；⑩数据库管理等。

6.8.3 部署专用安全系统和设备提升安全保护等级

面对企业级的安全保护需求，我们可以借助目前成熟的安全技术和产品来帮助提升整体安全保护等级。目前适合企业级的成熟的安全技术和产品有：

（1）Firewall 防火墙（首选网络版，备用单机版）；

（2）IDS 入侵检测（首选网络版，备用单机版）；

（3）VPN 虚拟专用网（首选 IPSEC 版，备用 SSL 版）；

（4）PKI/CA；

（5）防杀病毒（网关型，服务器型，桌面型）。

6.8.4 加强安全教育培训来减少和避免安全事件的发生

在整个安全体系建设中，人是最重要的因素，针对人所进行的安全培训也就成为了重要内容。安全培训内容包括：

（1）黑客攻击与防御相关技术；
（2）网络应用系统安全（网络设备、操作系统、应用服务）；
（3）安全产品技术与应用；
（4）信息安全管理体系；
（5）信息安全整体解决方案。

6.8.5　引入应急响应服务及时有效地处理重大安全事件

1．安全应急响应服务的特点

（1）技术复杂性与专业性

各种硬件平台、操作系统、应用软件。

（2）知识经验的依赖性

由计算机安全事件应急小组 CSIRT（Computer Security Incident Response Team）中的人提供服务，而不是一个硬件或者软件产品。

（3）突发性和时效性强

（4）需要广泛的协调与合作

2．应急事件

（1）大规模病毒爆发
（2）网络入侵事件
（3）拒绝服务攻击
（4）主机或网络异常事件

3．应急服务内容

（1）协助恢复系统到正常工作状态
（2）协助检查入侵来源、时间、方法等
（3）对网络进行评估，找出其他网络安全隐患
（4）做出事故分析报告
（5）跟踪用户运营情况

6.8.6　借助安全通告服务对安全威胁提前预警

安全信息通告包括以下内容：

（1）紧急事件通告；
（2）业界动态；
（3）最新技术发展；
（4）国家安全政策及法律法规。

只有积极主动地建立起一套完备的安全服务保障体系，才能够真正有效地解决安全问题，而不是仅仅依靠事后处理（应急响应）。

6.9　操作案例

解决局域网安全问题需要用多种方式来进行解决，其中主要的两种方式就是通过合理

配置提高系统安全性和安装监控管理软件来保证系统的安全，下面我们就这两个方面做一个简单的介绍。

6.9.1　通过配置来增强系统安全性

注册表中保存有计算机系统安全设置的大多数，通过注册表的合理配置可以增强计算机在局域网中的安全性。

1．隐藏计算机名

为了保护计算机上的资源不受其他人的非法访问和攻击，有时需要把局域网中指定的计算机名称隐藏起来，让其他局域网用户无法访问到。

具体的操作步骤如下。

（1）打开注册表编辑器，选择“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters”注册表键，如图 6-1 所示。

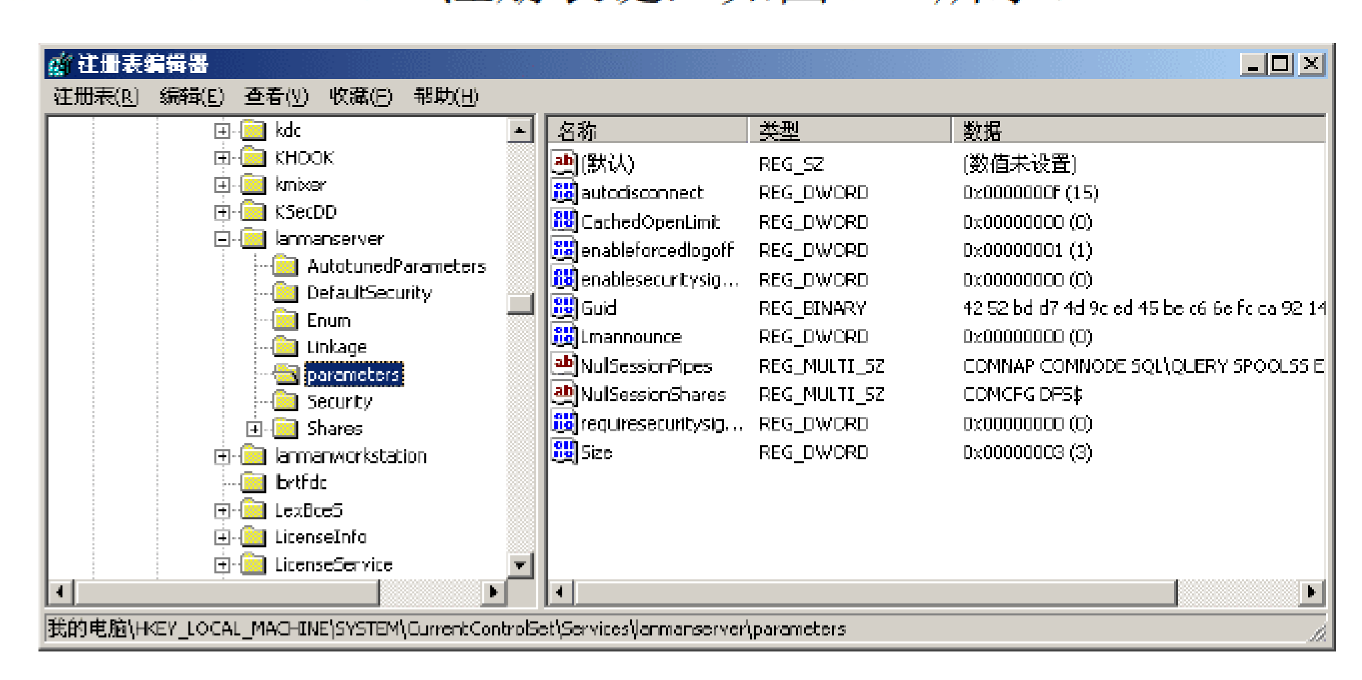


图 6-1　隐藏计算机名设置前

（2）用鼠标单击窗口右边的 Hidden 键名称，如果未发现此键名称，在窗口右边的空白处右击，从菜单中选择“新建”|“双字节值”命令，新建一个名称为 Hidden 的键，将其值设置为“1”，如图 6-2 所示。

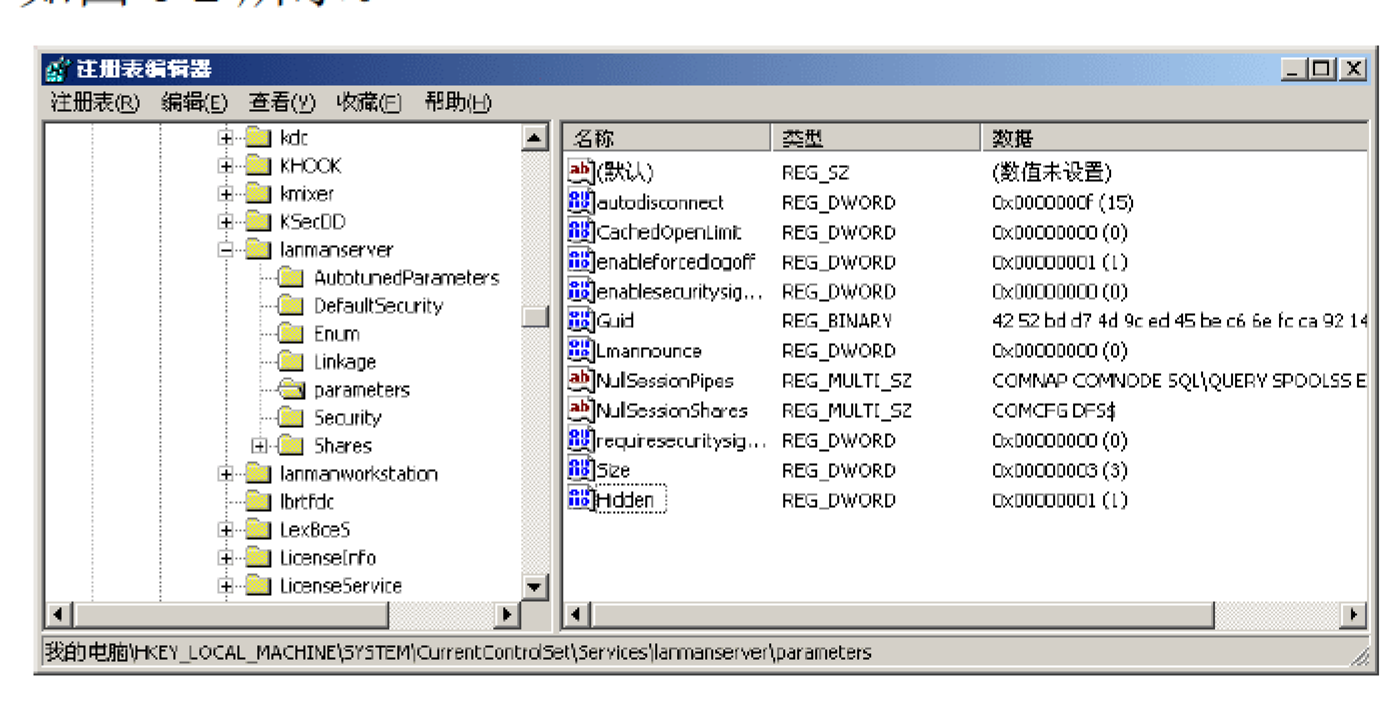


图 6-2　隐藏计算机名设置后

（3）关闭注册表编辑器，然后重新启动计算机以后，该计算机就被隐藏了。

2．防止其他人非法编辑注册表

计算机的大量安全设置都在注册表中，所以保护好注册表中的设置，防止非法对注册表进行任意修改是提高安全性的一个重要内容。

具体方法如下。

（1）打开注册表编辑器，选择“HKEY_CURRENT_USER\Software\Microsoft\ Windows\

CurrentVersion\Policies”注册表键，如图 6-3 所示。

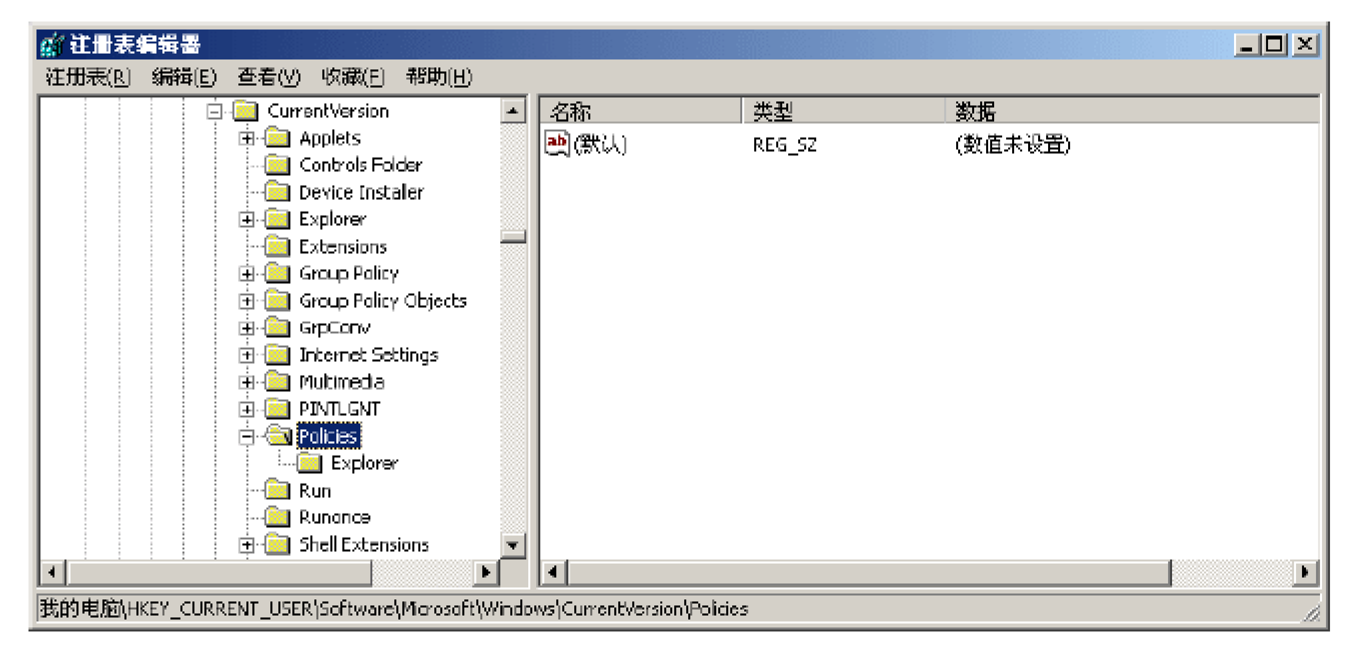


图 6-3　禁止访问注册表前

（2）在 Policies 键值的下面新建一个名为 System 的主键，右击 Policies 键，在弹出的菜单中选择“新建”|“项”命令，将新建的键名称设置为 System，如图 6-4 所示，如果该主键已经存在的话，可以直接进行下一步。

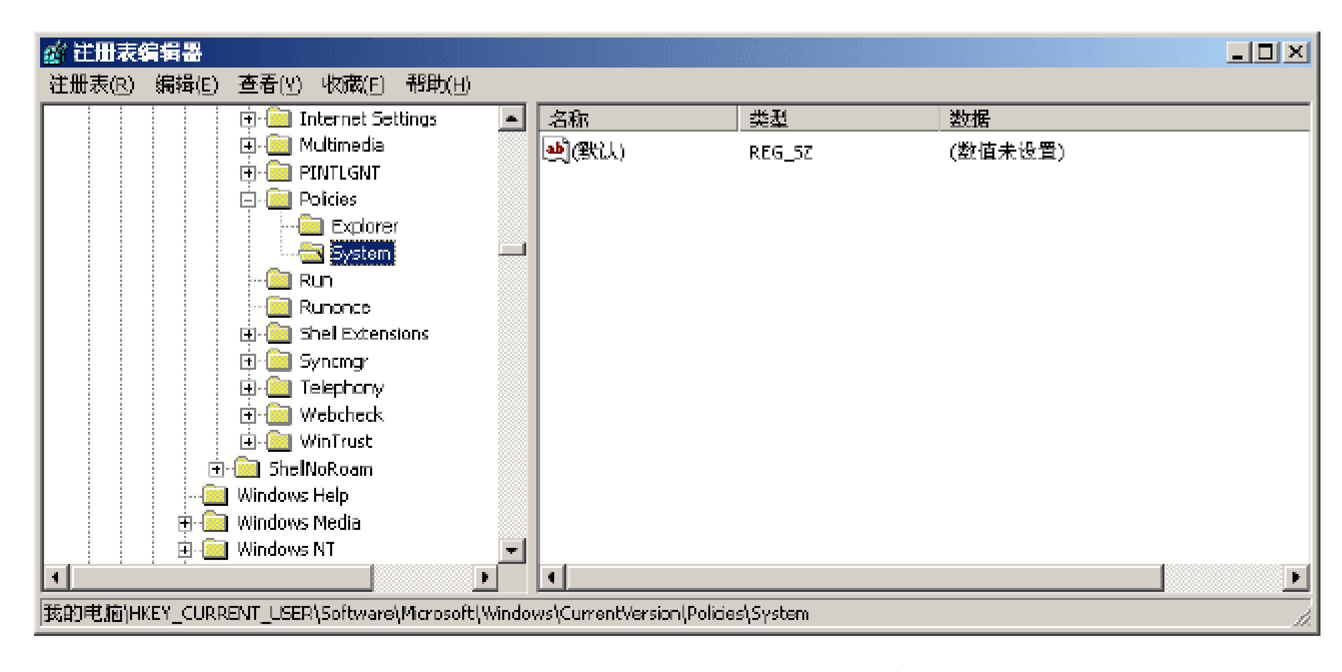


图 6-4　添加 System 键窗口

（3）选择新建立的 System 键，在右边窗口的空白处右击，再弹出的菜单中选择“新建”|“双字节值”命令，新建一个 DWORD 串值，设置其名称为 DisableRegistryTools，设置其值为“1”，如图 6-5 所示。

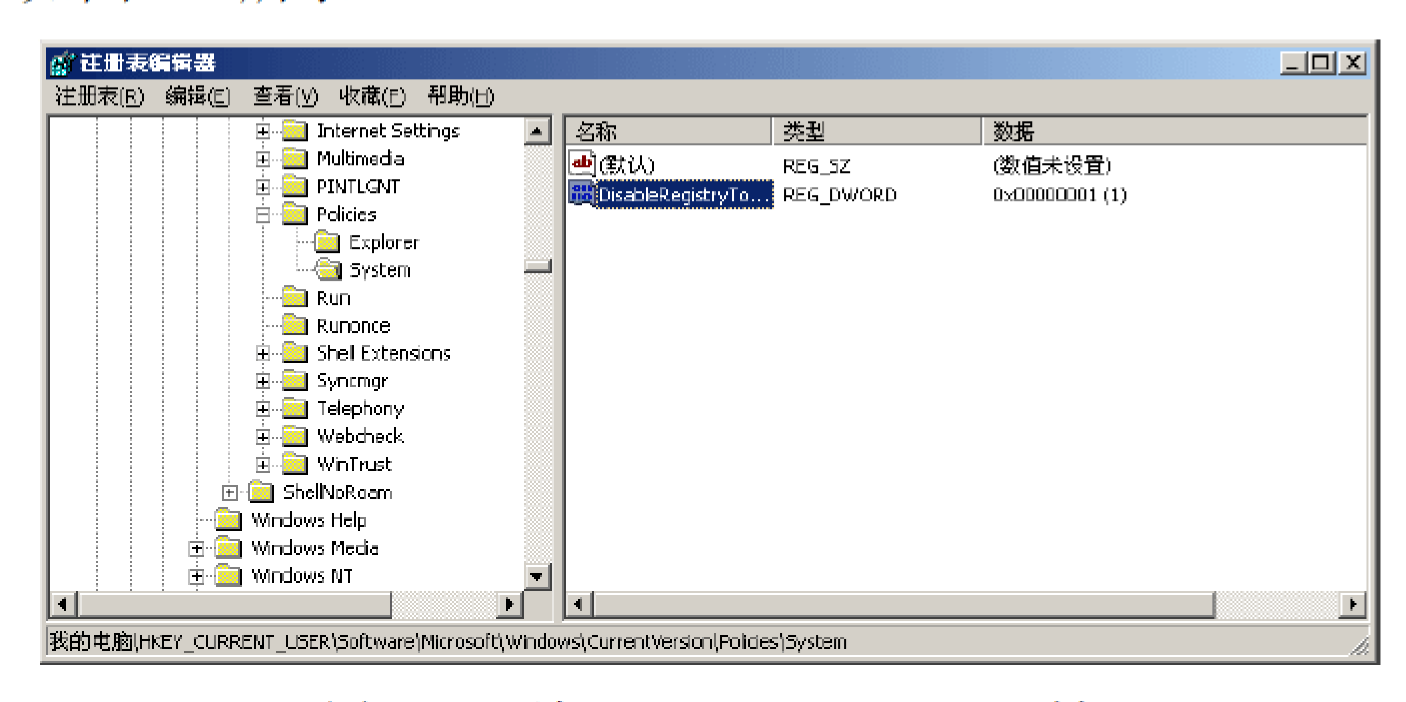


图 6-5　添加 DisableRegistryTools 键

（4）设置好以后，重新启动计算机就可以达到防止其他人非法编辑注册表的目的了。

3．禁止对控制面板的访问

控制面板中涉及到计算机系统的安全设置，防止非法修改控制面板设置对提高系统安全性具有重要意义。

具体的操作方法如下。

（1）打开注册表编辑器，选择“HKEY_CURRENT_USER\Software\Microsoft\ Windows\

CurrentVersion\Policies\System”注册表键，如图 6-6 所示。

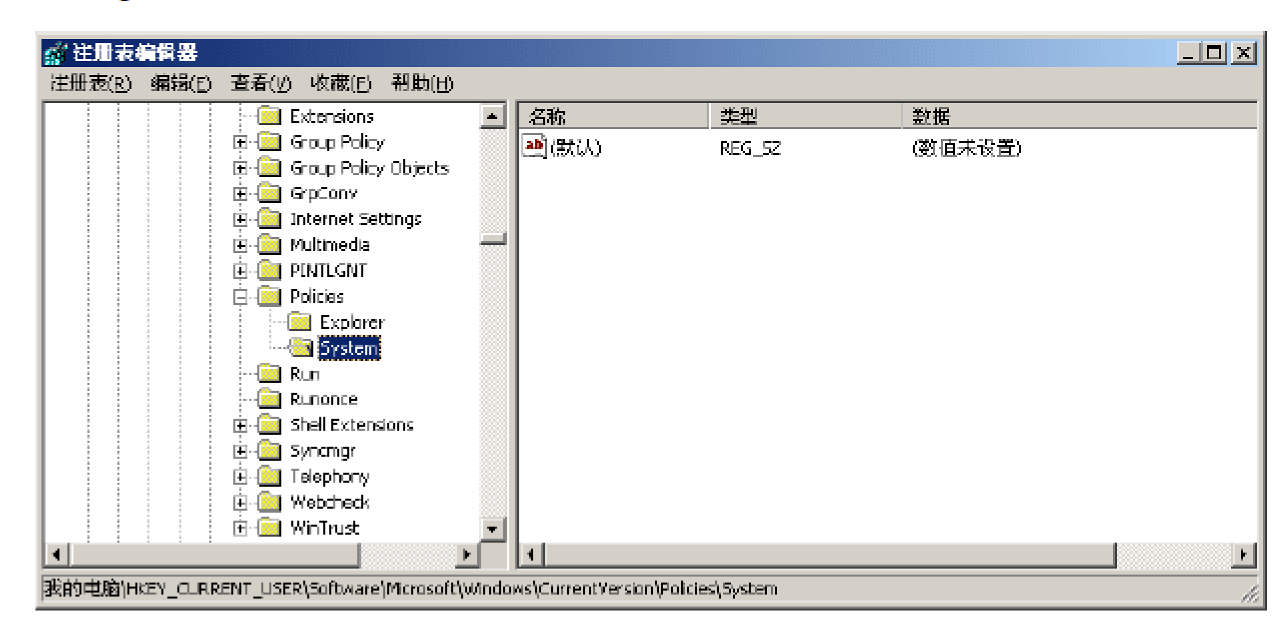


图 6-6 禁止对控制面板的访问前

（2）在窗口右边的空白部分右击，在弹出菜单中选择“新建”|“双字节值”命令，将新键名称设置为 NoDispCPL，将其值设置为“1”，如图 6-7 所示。

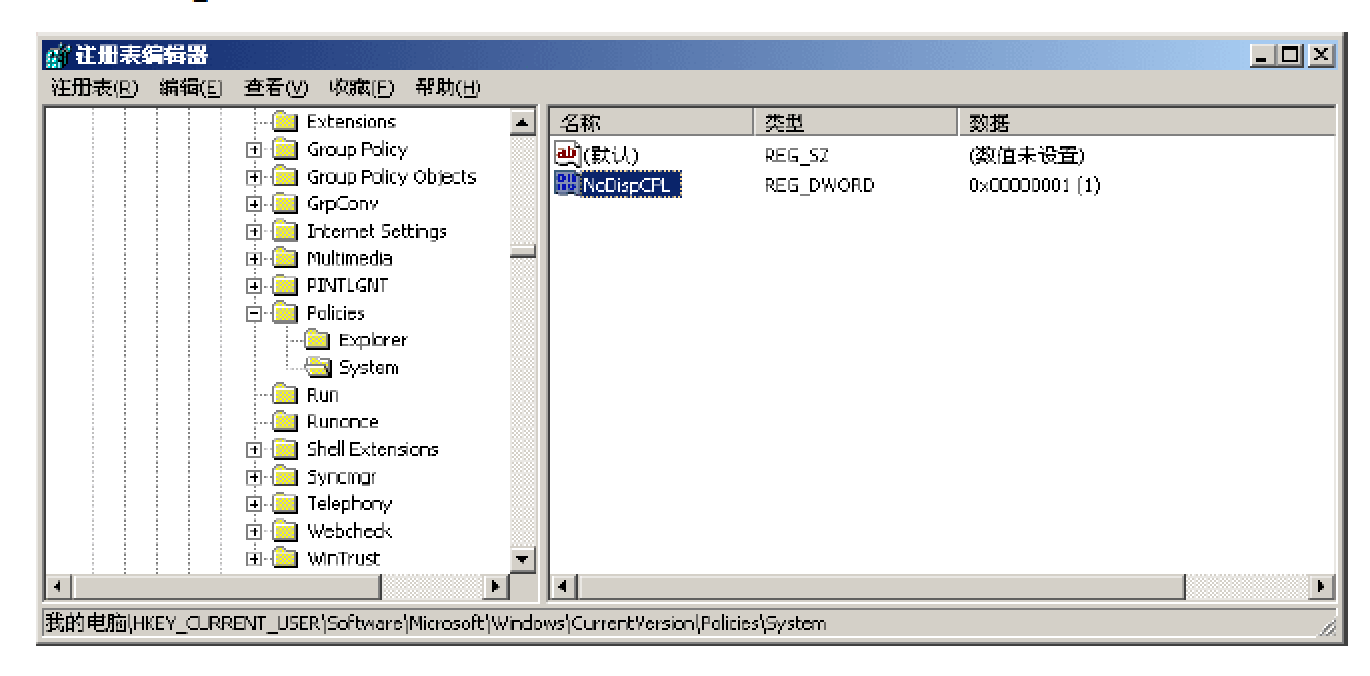


图 6-7 禁止对控制面板访问后

（3）关闭注册表编辑器，重新启动计算机，控制面板被禁止访问了。

4．禁止拨号访问

局域网内的计算机安全性可能不是很高，通过拨号与外部网络进行连接时，得不到企业防火墙的保护，所以很容易引入安全问题，所以尽量避免通过拨号来访问外部网络。

（1）打开注册表编辑器，选择“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies”注册表键，如图 6-8 所示。

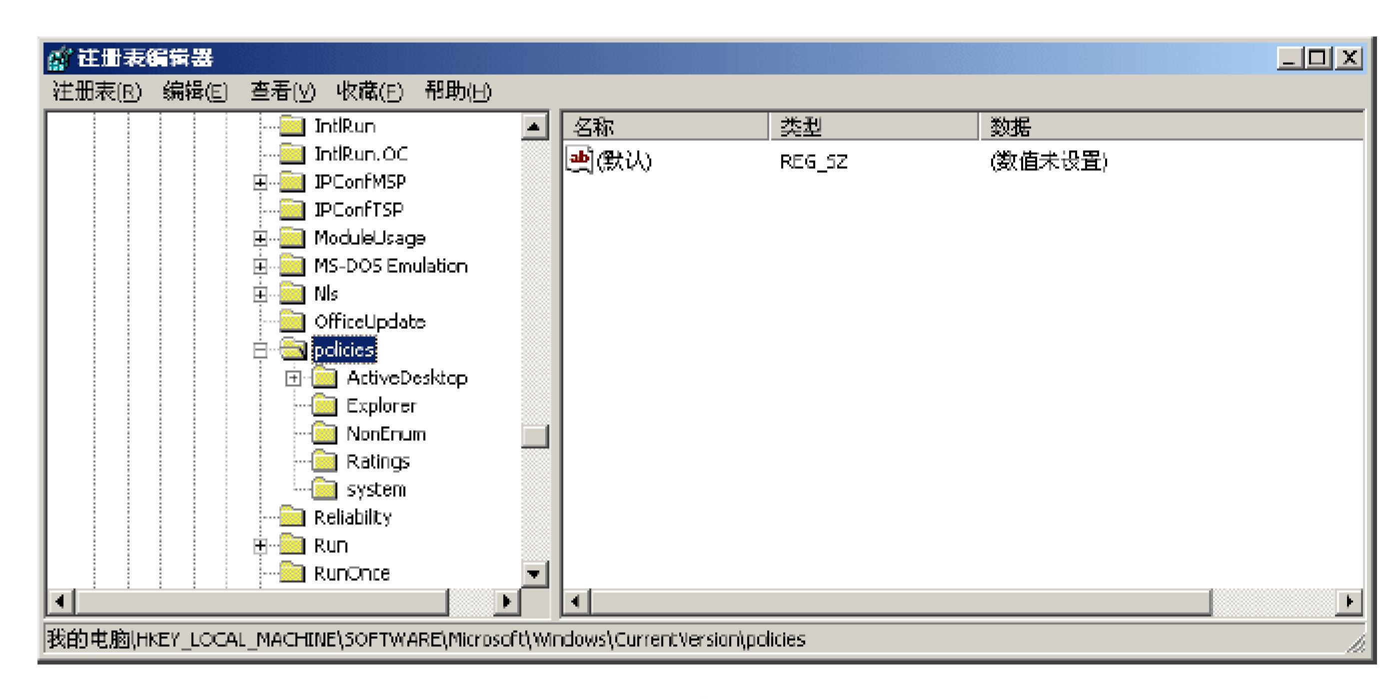


图 6-8 禁止拨号前

（2）右击 Policies，在弹出的菜单中选择“新建”|“双字节值”命令，将新建的键名称设置为 Network，在窗口右边的部分右击，在弹出的菜单中选择“新建”|“双字节值”命令，将键名称设置为 NoDialIn，其对应的值为 0 表示禁止拨号，为 1 表示允许拨号，所以将其值设置为“0”，如图 6-9 所示。

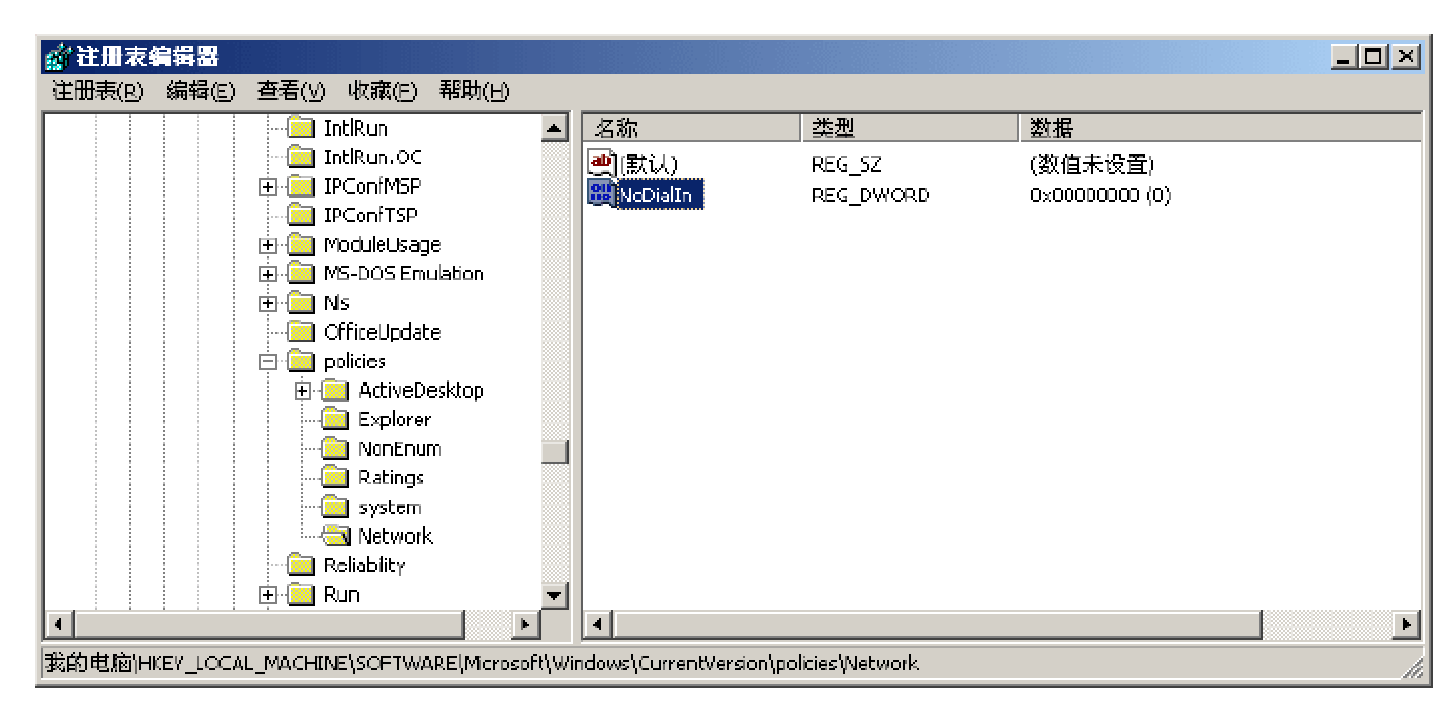


图 6-9　禁止拨号访问设置

（3）关闭注册表编辑器，重新启动计算机，拨号访问的功能就被禁止了。

5．只允许运行特定程序

计算机系统的安全问题，有相当一部分都是运行了某个非法程序而造成的，所以为了计算机系统的安全，限定用户只能运行一些安全的程序可以有效提高系统的安全性。

操作步骤如下。

（1）打开注册表编辑器，选择“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer”键，如图 6-10 所示。

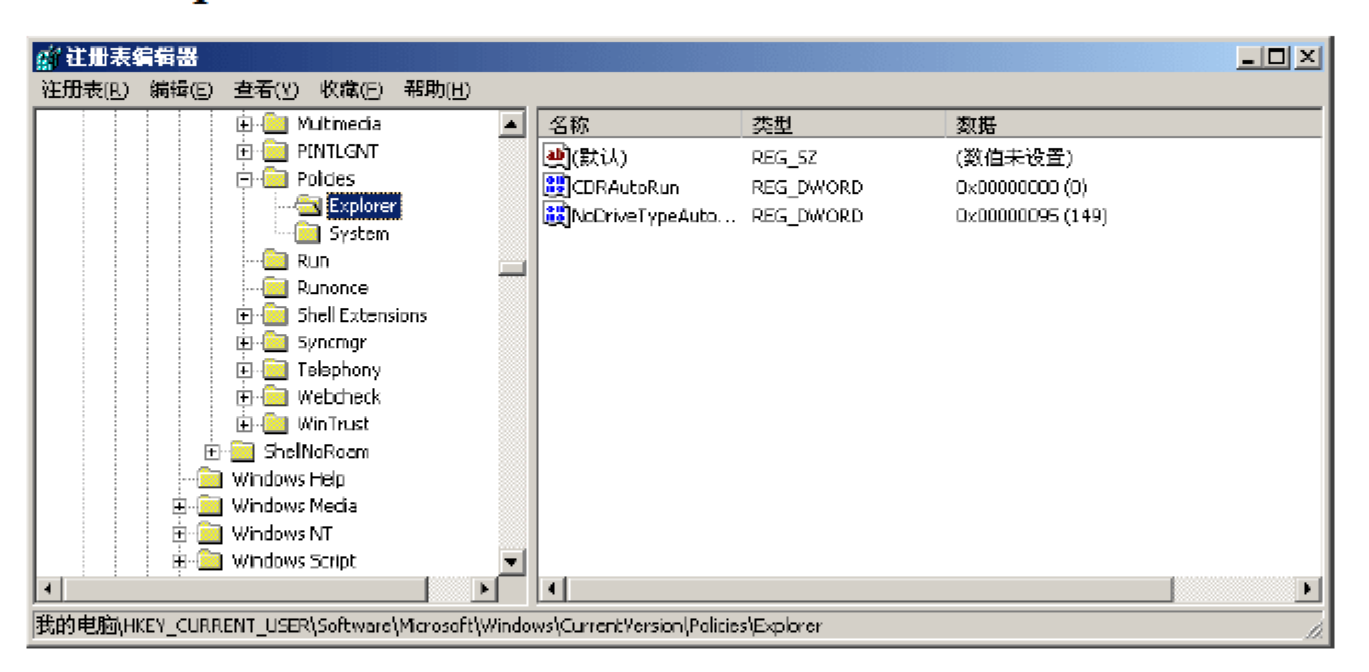


图 6-10　禁止运行程序设置前

（2）右击窗口左边的 Explorer 项，在弹出菜单中选择“新建”|“项”命令，设置项的名称为 RestrictRun，然后在窗口右边空白处右击，从弹出菜单中选择“新建”|“字符串”命令，将其名称设置为“1”，其值设置为 NotePad.exe，如图 6-11 所示。

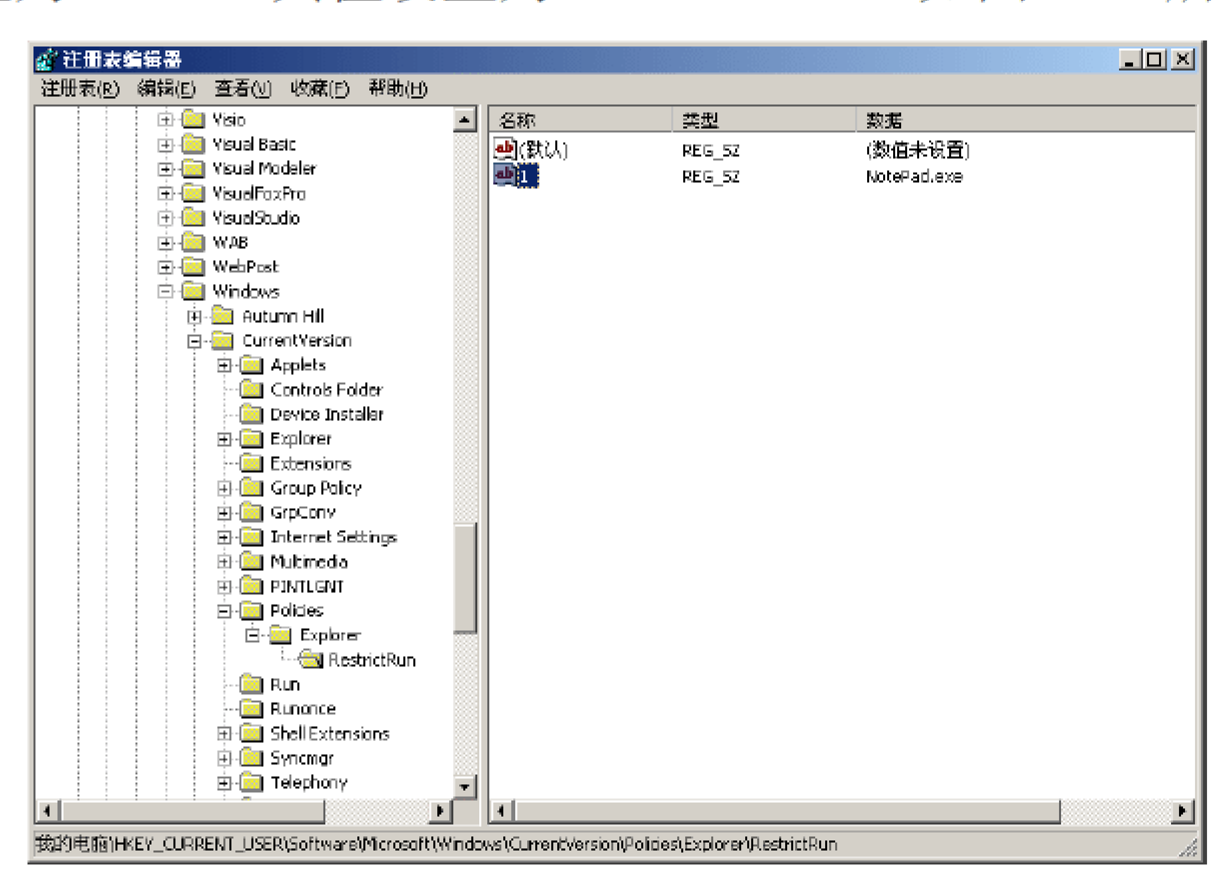


图 6-11　新建字符串

（3）设置完成后，重新启动计算机，就只有设置的程序才能运行，而不能运行其他的非法程序，让计算机的安全得到保障。

提示： 当限制非法程序运行时，设置的项目中要包含常用的程序，比如注册表编辑器 regedit.exe，这样当需要修改或者添加时才能方便地进行，不然会比较麻烦。

6.9.2 计算机外设管理

计算机外设（包括光驱、软驱、USB 接口、打印机、刻录机、串口、并口等）作为计算机对外信息交换的通道，这些外设为计算机与外界进行信息交换提供了非常方便的途径，比如一张普通刻录光盘容量达 600 多 MB，移动硬盘的容量都在几十 GB，甚至上百 GB，通过将计算机接入企业内部网络复制文件等，通过这些途径，足以将企业内的所有重要文件资料复制带出企业，所以对企业局域网中计算机的外设进行有效管理具有重要意义。下面我们以北京世优时代科技有限公司开发的一款计算机外设管理软件来进行说明。

具体的操作过程如下。

（1）选择“开始”|“程序”|“计算机外设监控系统”|“设备控制服务器”命令，出现程序主窗口，如图 6-12 所示。

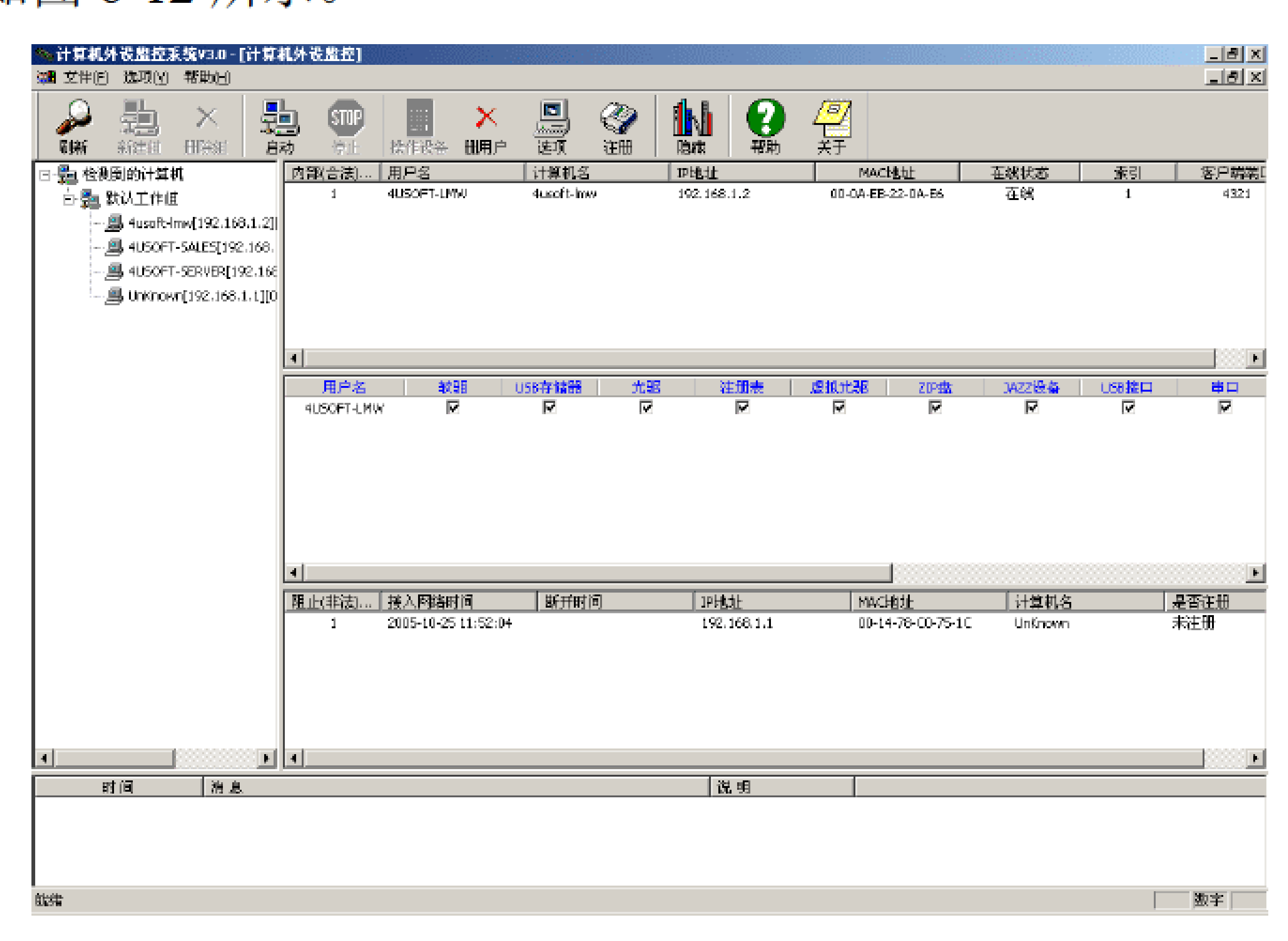


图 6-12 设备控制服务器主界面

（2）双击窗口右侧的计算机列表项，可以看到该计算机的外设状态并可以对该计算机对应的外设进行操作（启用或禁止），如图 6-13 所示。

（3）在外设设置窗口中，取消“串口”复选框的选择，就达到禁止该计算机使用串口进行通信的目的，然后单击“确定”按钮。右击桌面上的“我的电脑”，从弹出菜单中选择“属性”命令，在出现的“系统特性”对话框中选择“硬件”选项卡，单击“设备管理器”按钮，出现“设备管理器”窗口，可以看到串口已经被禁止使用，如图 6-14 所示。

（4）通过该系统对局域网中的计算机外设进行控制，可以非常方便地随时根据工作的需要开启对应的外设接口进行使用，使用完成后再对其禁止。

（5）单击工具栏上的“启动”按钮，可以禁止外部计算机接入企业内部网络，在窗口右侧最下面的列表中显示的就是非法接入企业内部网络的计算机，系统会提示有非法计算机的同时阻止该计算机接入内部网络，如图 6-15 所示。

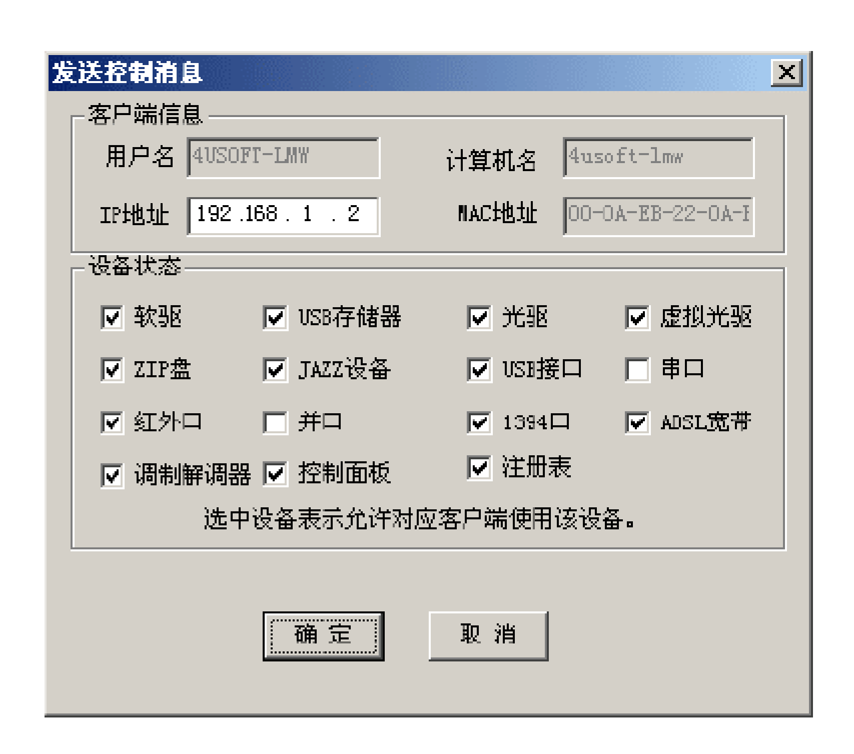



图 6-13　外设状态设置窗口

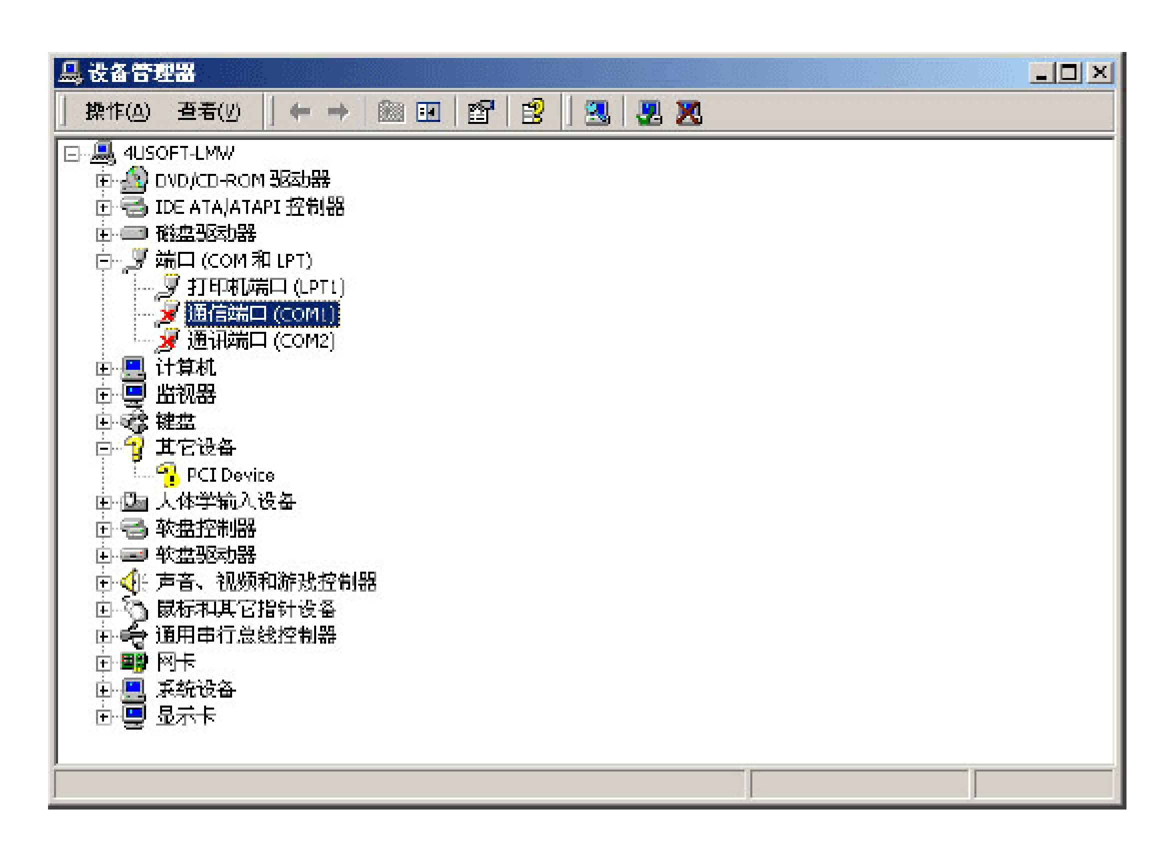


图 6-14　“设备管理器”窗口

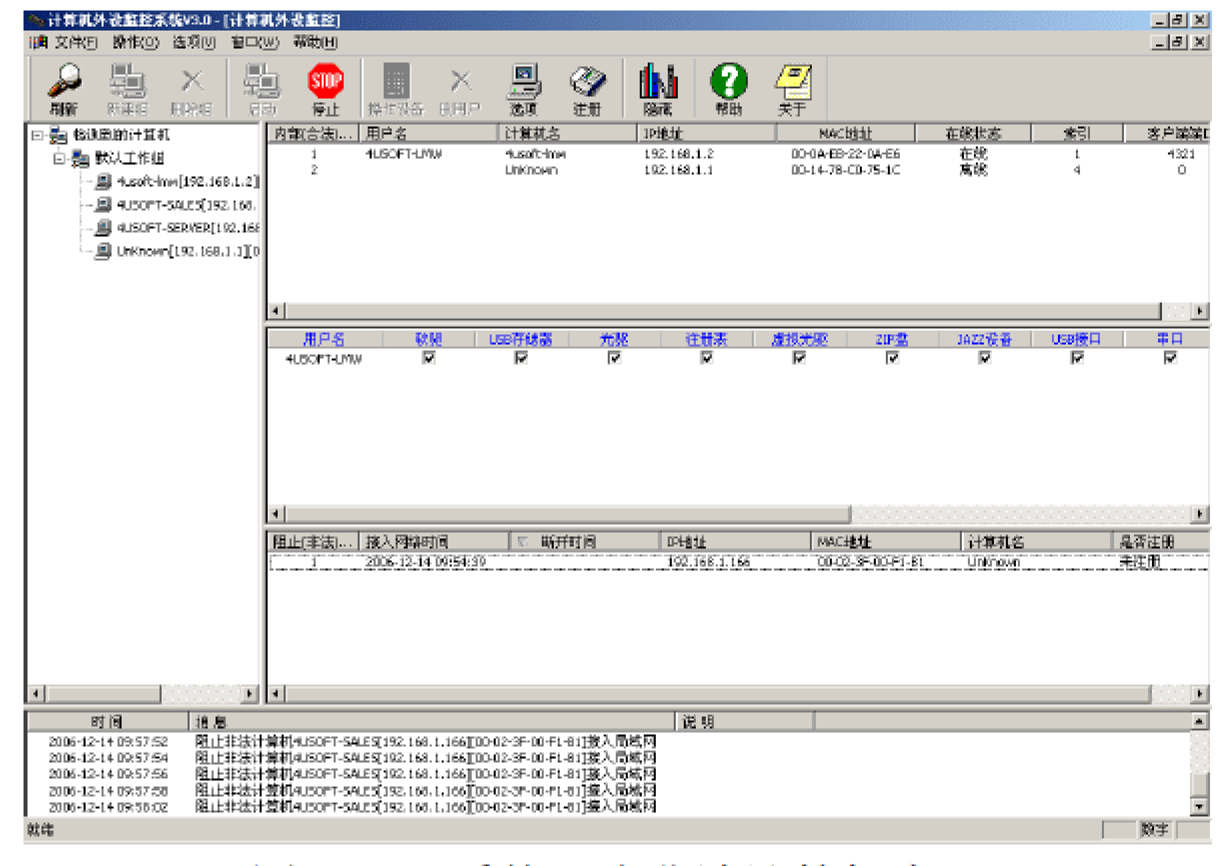


图 6-15　系统阻止非法计算机窗口

（6）当因工作需要接入外部计算机的时候，可以通过右击非法计算机，从弹出菜单中选择“设置为合法”命令，就可以将该计算机设置为合法计算机，系统就不会阻止该计算机接入网络进行工作，注意当工作完成的时候，一定要将该计算机设置为非法。另外，还可以将该计算机设置为临时合法，分配一个固定的时间，比如 30 分钟，时间到达的时候，系统自动再将其设置为非法。

（7）当系统安装完成的时候，首先需要配置的就是内部计算机，否则所有的计算机都会作为外部计算机来对待，就会被阻止接入网络。单击工具栏窗口上的“选项”按钮，出现“参数设置”对话框，选择“内部计算机”选项卡，如图 6-16 所示。

（8）单击“添加”按钮，出现“添加合法计算机”对话框，如图 6-17 所示。

（9）在“添加合法计算机”窗口中，“计算机信息”列表框中显示了系统扫描局域网得到的计算机信息，可以选择列表中的计算机，也可以直接输入计算机信息来添加合法的计算机，设置完成后，单击“确定”按钮，符合指定信息的计算机就会被添加到合法计算机列表中。

提示： 如果知道需要添加的计算机的 IP 信息，而不知道其 Mac 地址和计算机名，在该计算机接入网络的情况下，可以在“IP 地址”文本框中填入 IP 地址，然后单击“Mac 地址”文本框后面的“自动”按钮，而得到 Mac 地址，单击“计算机名”文本框后面的“自动”按钮得到该计算机的计算机名。





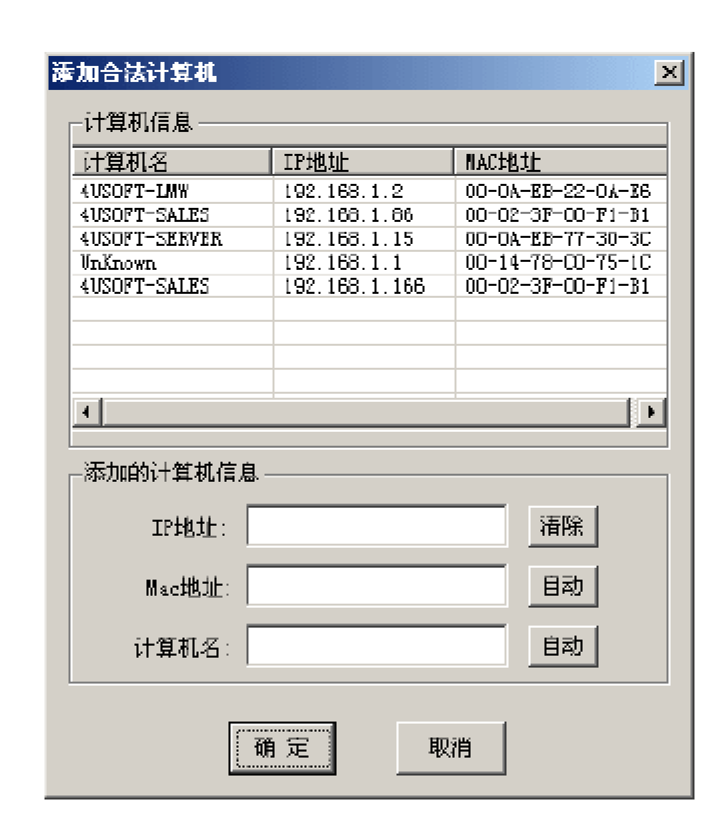


图 6-16　内部计算机设置窗口　　　　图 6-17　“添加合法计算机”对话框

（10）选择主窗口上的“文件”|“设备日志”命令，可以看到系统中计算机外设使用状态的改变情况，如图 6-18 所示。

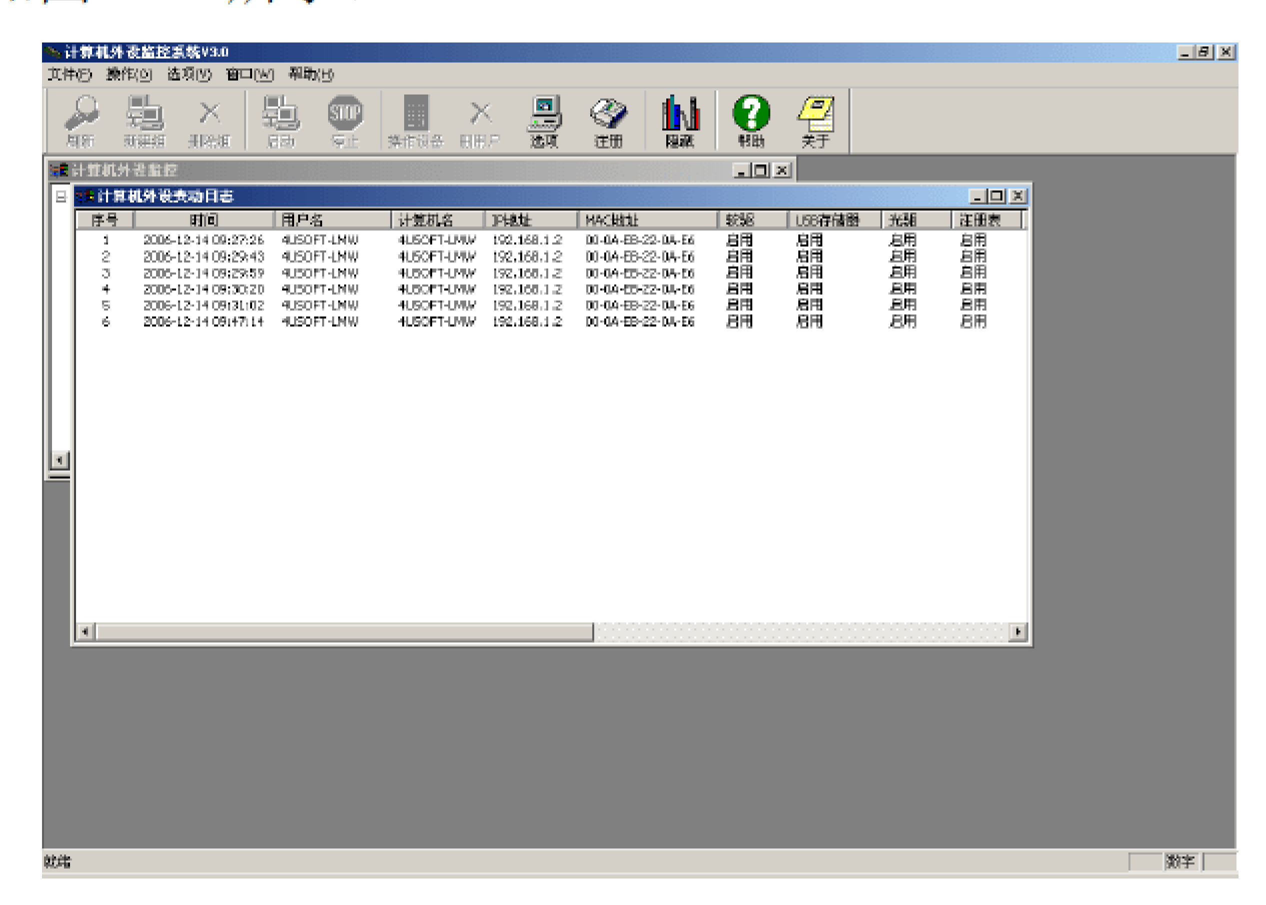


图 6-18　计算机外设变动日志

（11）选择主窗口上的“文件”|“电脑”命令，可以看到接入和断开系统网络的计算机信息，以便了解有哪些计算机接入到企业内部网络中，如图 6-19 所示。

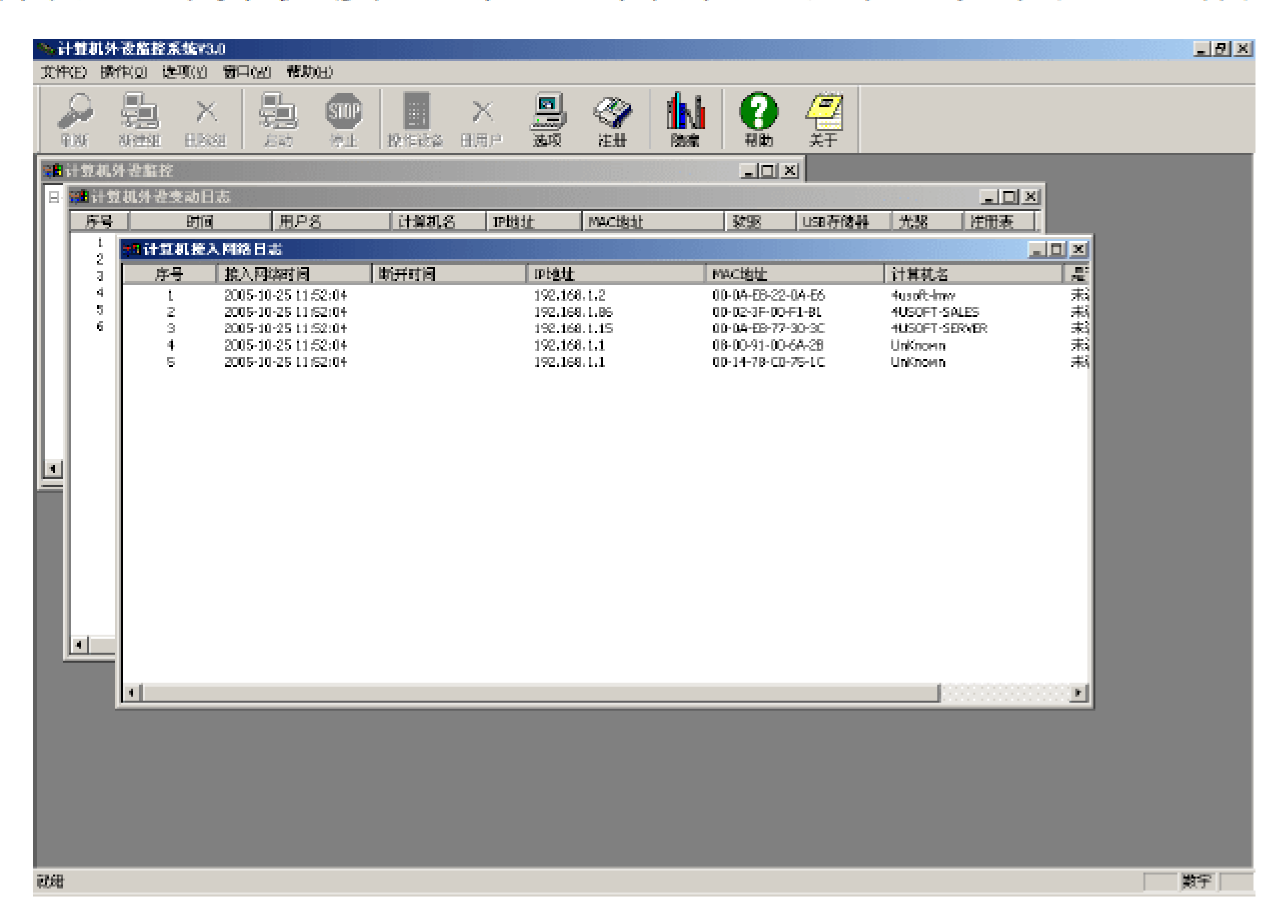


图 6-19　计算机接入网络日志信息

（12）通过该系统可以实现对局域网内计算机外设使用状态和外部计算机接入内部局域网的情况进行监控。

6.9.3　局域网资产管理

局域网中的资产包括硬件资产和软件资产，通过专门的软件系统对这些资产进行管理不仅可以大大提高管理效率，而且还能为企业的信息化发展提供相关依据，下面我们以北京世优时代科技有限公司开发的一款资产管理软件来进行说明。

具体操作步骤如下。

（1）选择“开始”|“程序”|“网络综合管理信息系统”|“网络资产管理系统”命令，出现资产管理系统主窗口，如图 6-20 所示。

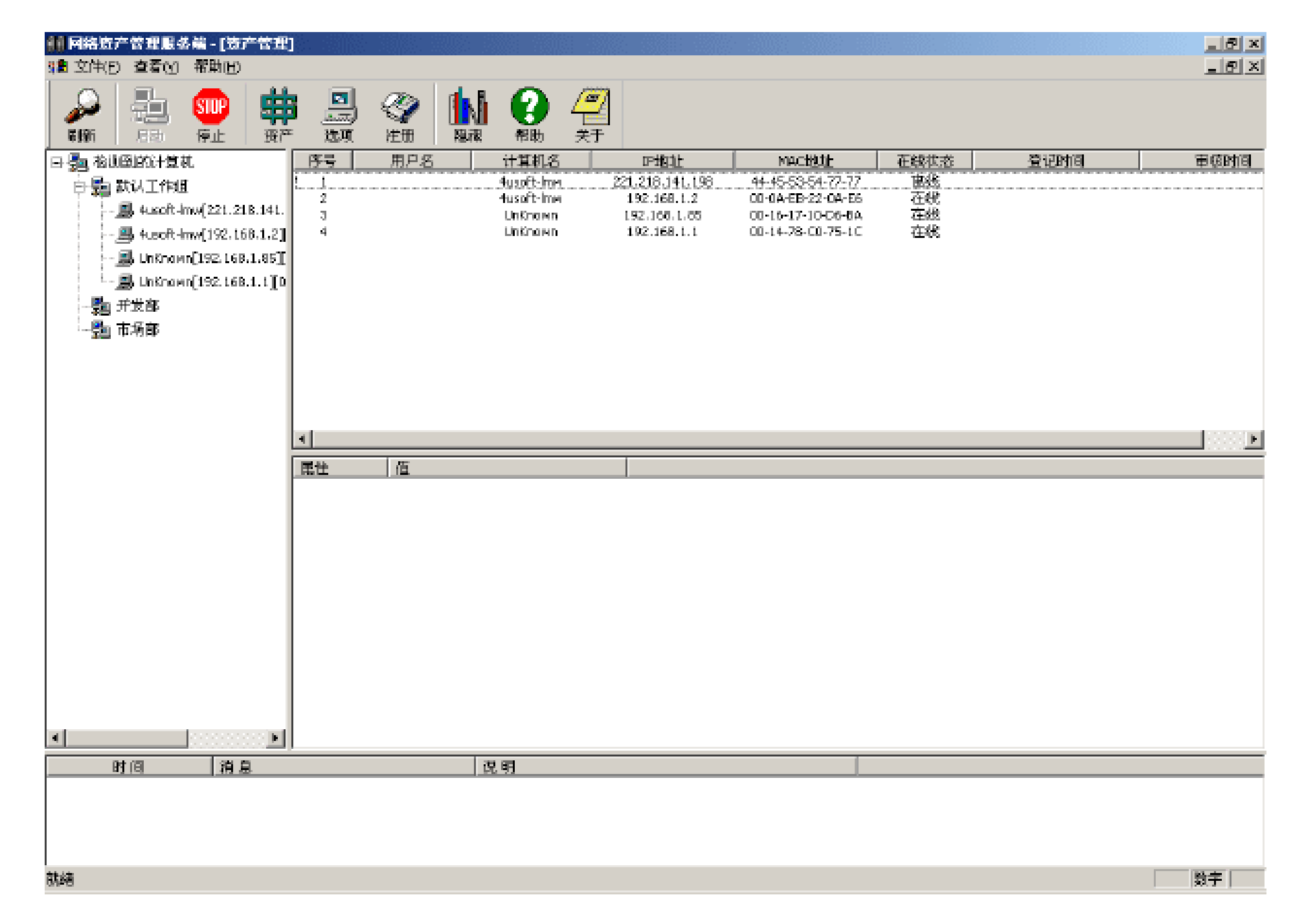


图 6-20　资产管理系统主窗口

（2）单击工具栏上的“刷新”按钮，系统可以自动扫描局域网内的计算机，并将扫描到的计算机信息显示在右边的窗口中。选择一条记录，右击该记录，从弹出的快捷菜单中可以选择“远程安装”、“远程卸载”、“获取资产”、“更新配置”、“查看文件”5 种操作。

（3）选择“远程安装”命令，弹出要求输入用户名和密码的窗口，如图 6-21 所示。

（4）在窗口中输入用户名和密码，单击“确定”按钮，出现新窗口，要求数据特定客户端计算机的信息，如图 6-22 所示。

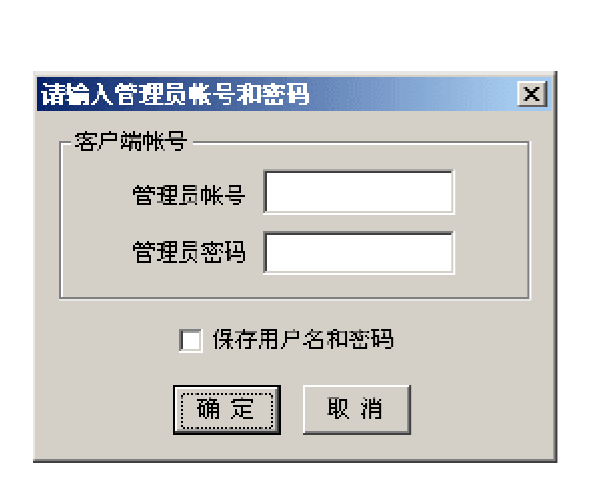


图 6-21　输入客户端管理员账号



图 6-22　客户端计算机信息窗口

（5）输入相关信息后，单击“继续”按钮，完成对客户端的自动安装并第一次将客户端的数据上传到服务器端，从窗口最下面的日志信息中可以看到安装信息，如图 6-23 所示。

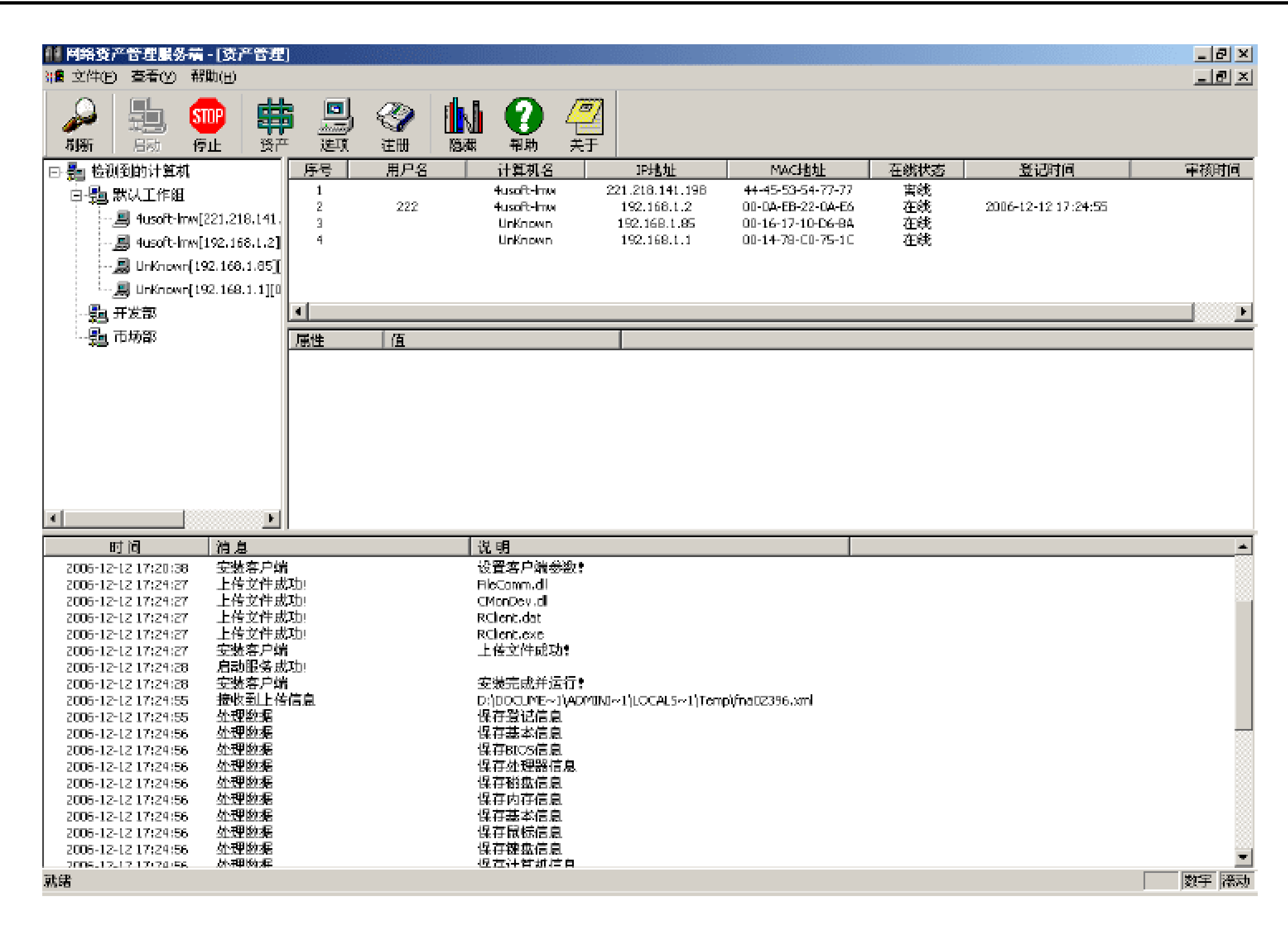


图 6-23 客户端安装信息

（6）在右边窗口中选择刚才已经完成客户端安装的计算机，然后单击工具栏上的“资产”按钮，出现该计算机的资产查看窗口，如图 6-24 所示。

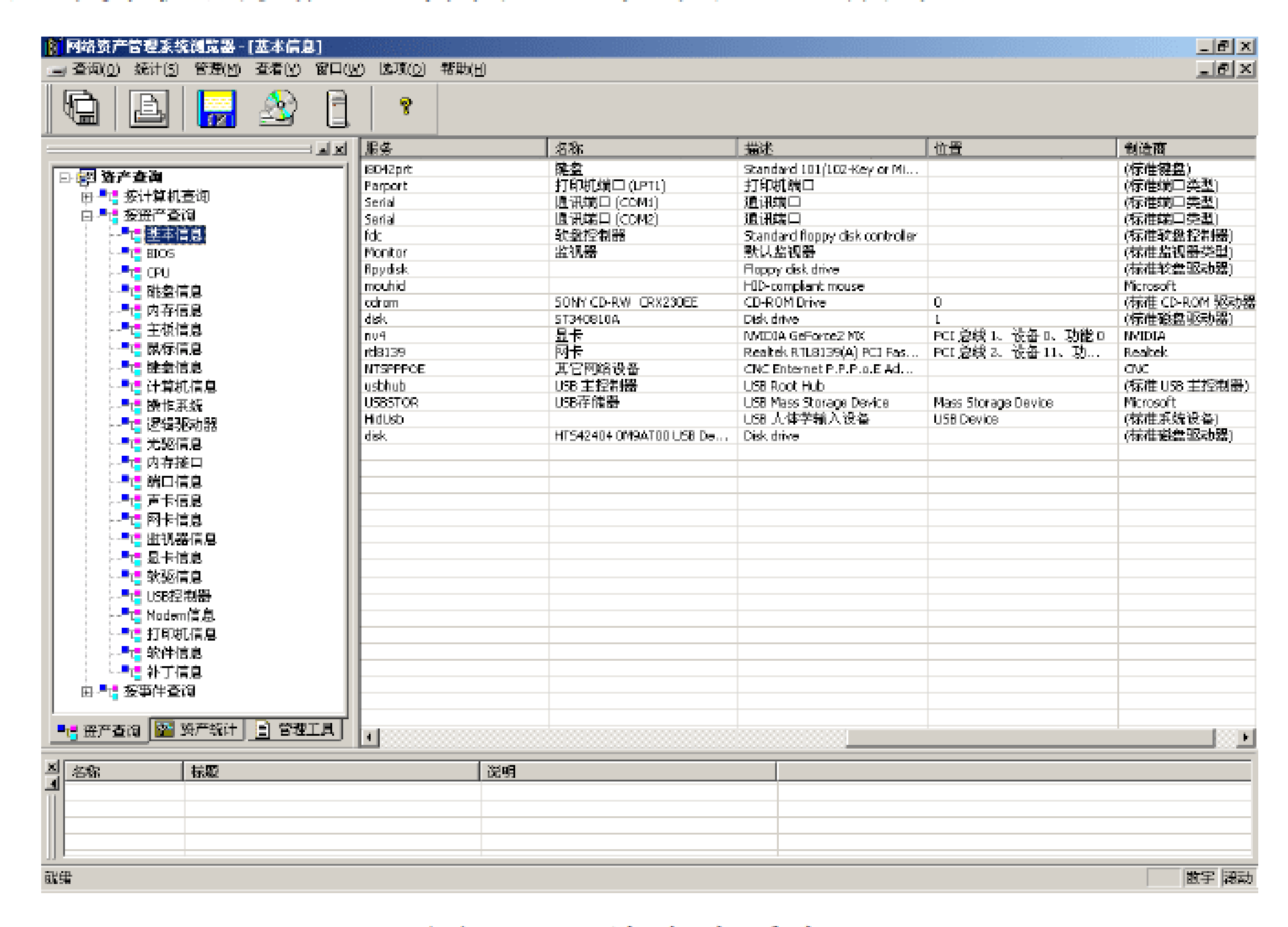


图 6-24 资产查看窗口

（7）在资产查看窗口中，可以对系统中的资产按照不同的分类进行查询，比如按计算机、按资产类型、按事件类型（主要记录局域网中资产变动情况）进行查询。

（8）双击窗口左边的“按计算机查询”，弹出查询条件设置对话框，如图 6-25 所示。

（9）设置好查询条件以后，单击“确定”按钮，在“按计算机查询”项下面的几项中显示的内容都是按照这里的条件进行的。

（10）双击窗口左边的“按资产查询”，弹出查询条件设置对话框，如图 6-26 所示。

（11）设置好查询条件以后，单击“确定”按钮，在“按资产查询”项下面的几项中显示的内容都是按照这里的条件进行的。

（12）系统除了提供查询功能以外，还提供了多种统计功能，单击窗口左边的“资产统计”选项卡，通过展开窗口上的树行项目可以看到系统的统计功能。如图 6-27 所示。



图 6-25　按计算机查询资产

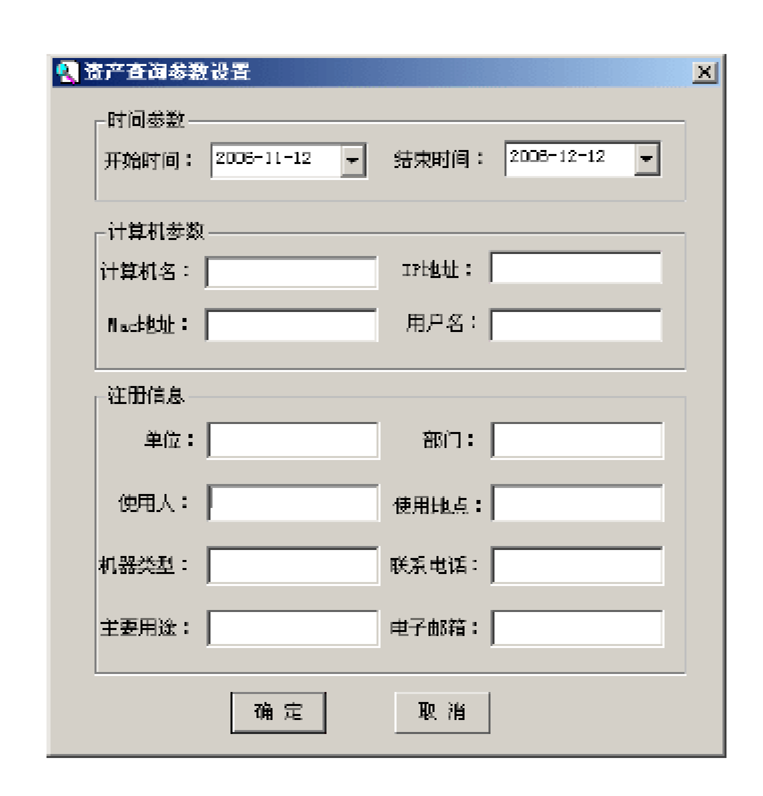


图 6-26　按资产查询条件设置

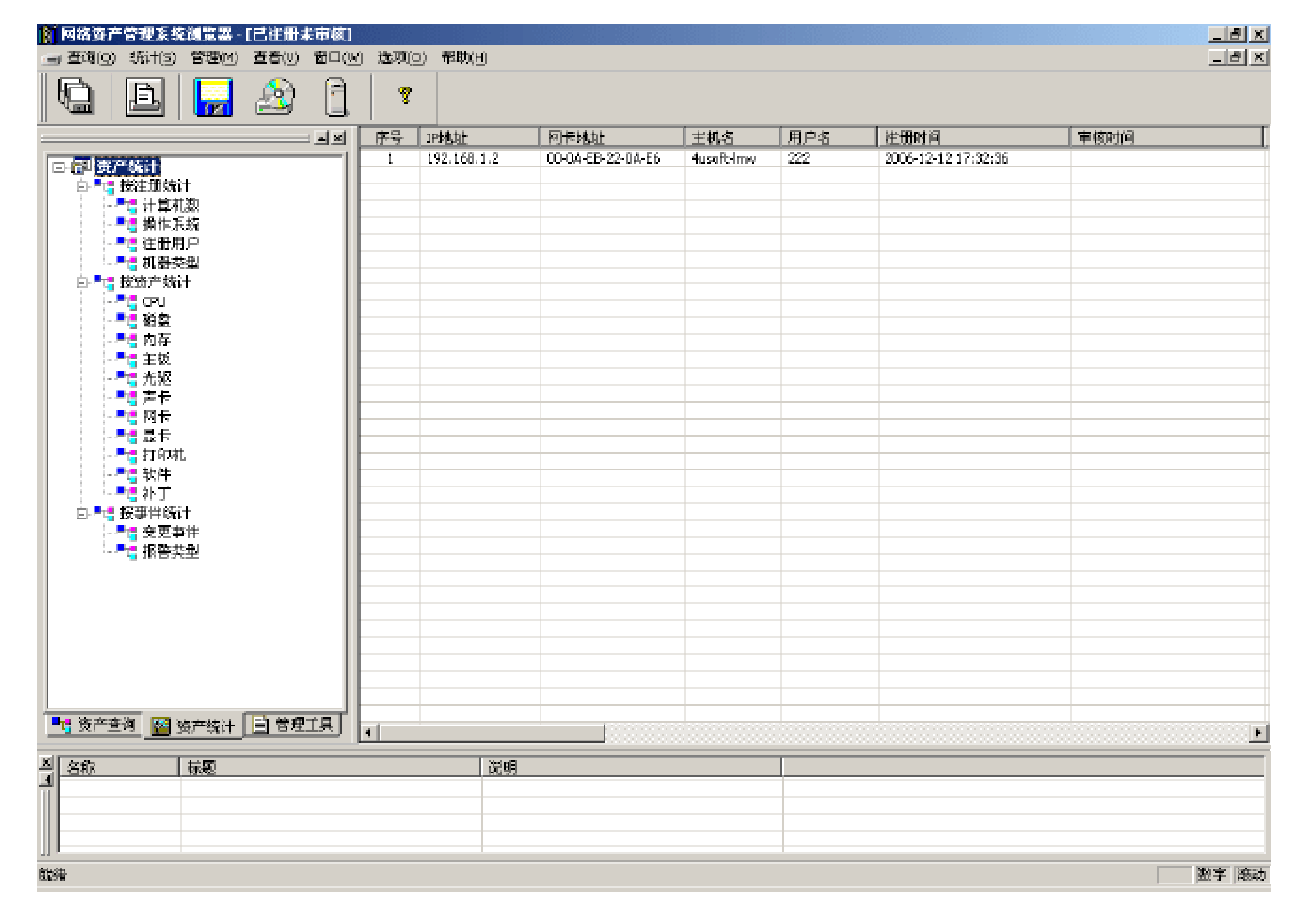


图 6-27　资产统计窗口

（13）通过双击资产统计项目即可完成对应的统计，并将统计结果显示在右侧的窗口中，选择“资产统计”|“按资产统计”|“补丁”并双击，统计信息将显示在窗口右侧，如图 6-28 所示。

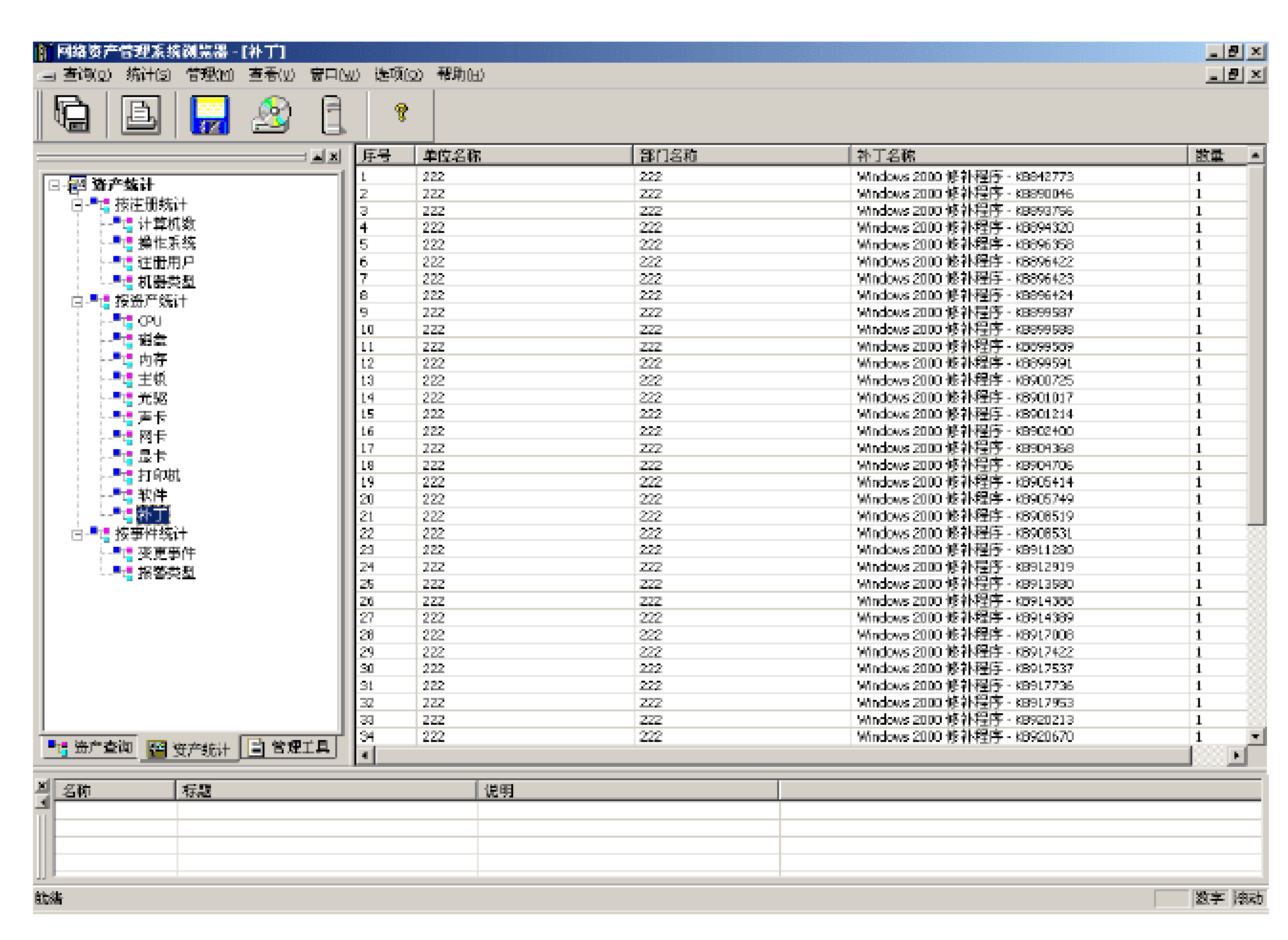


图 6-28　补丁统计信息

（14）系统提供了几项管理功能，包括“资产盘点”、“报表输出”、“数据导入”、“数据导出”、“数据备份”，单击左边窗口下面的“管理工具 ”选项卡，可以看到管理

工具的几个具体项目，如图 6-29 所示。

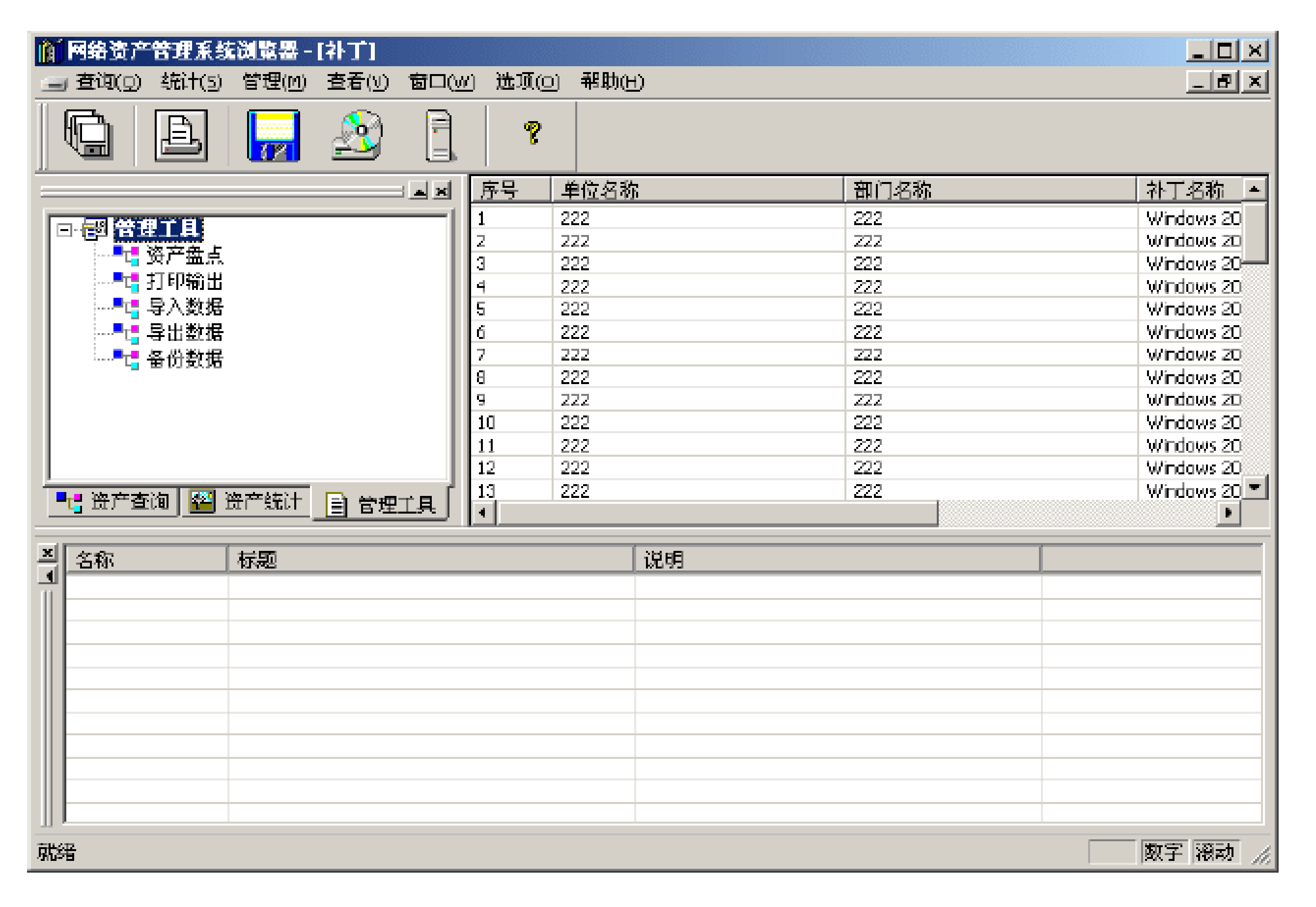


图 6-29　管理工具窗口

（15）双击“管理工具”窗口中的“导出数据”，出现导出文件路径和文件名设置对话框，如图 6-30 所示。

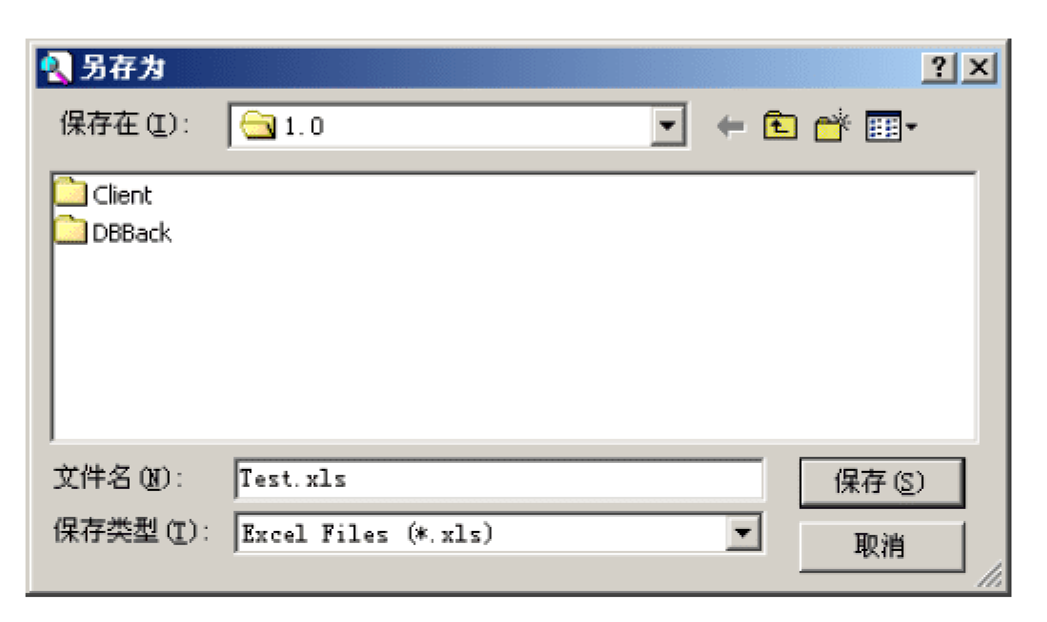


图 6-30　设置导出文件路径和文件名的对话框

（16）设置完成后，单击“保存”按钮，右边窗口中的内容全部被导出到了 Excel 文件中，可以进行更加灵活的处理，如图 6-31 所示。

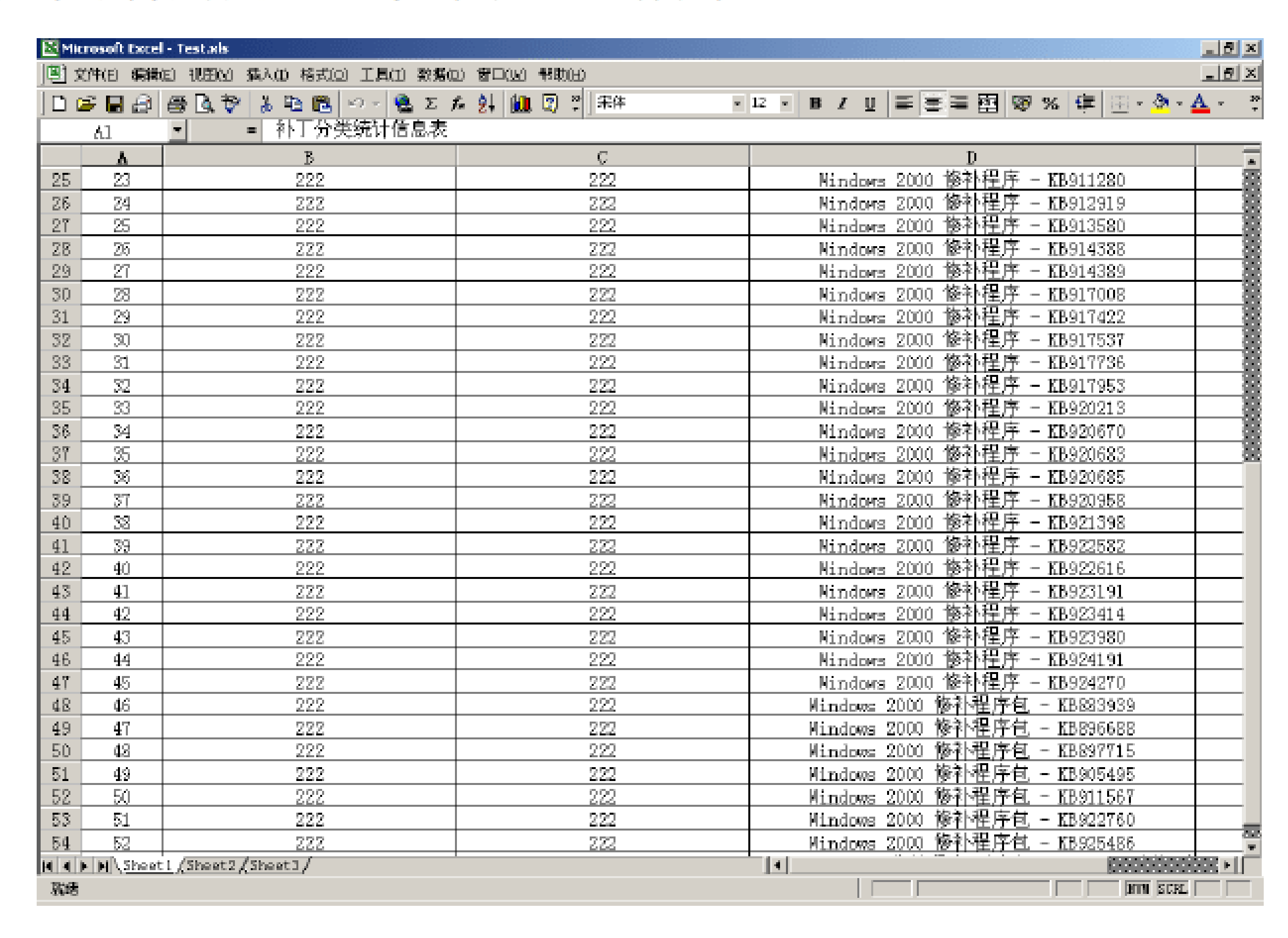


图 6-31　导出 Excel 窗口中的数据

至此，我们对该软件的基本功能就介绍完了，有些内容没有做详细的介绍，读者可以将没有介绍的部分进行练习，比如打印输出等。

习题

1. 简述安全评估在网络安全规划中的作用。
2. 简述网络系统面临的风险主要包括哪些。
3. 简述网络安全方案的设计原则。
4. 简述网络安全体系结构包括哪些内容。
5. 简述网络安全技术及其应用情况。
6. 简述无线局域网的安全问题及解决办法。
7. 简述网络安全服务的内容。

第 7 章　广域网安全管理

教学提示

目前世界上规模最大的计算机广域网是 Internet 网（即国际互联网），本书所讨论的广域网安全管理就是基于 Internet 网的网络安全管理。近年来，Internet 网取得了飞速的发展，通过提供丰富的网络服务，吸引了大量的网络用户，这些用户包括政府部门、工商企业、学校、医院和个人，同时网络安全事故频繁出现，从一定程度上阻碍了其发展。

本章将从广域网的发展、广域网的应用、广域网安全重要性以及广域网可能面临的安全风险和相关的安全技术进行探讨。特别对跨广域网的企业信息系统、电子商务、电子政务所面临的安全挑战和解决方案进行了探讨。

通过对本章的学习，应当充分掌握广域网安全的重要性，清楚广域网面临的各种安全风险，掌握各种广域网信息安全技术的基本知识。理解要进一步发展基于广域网的应用，做好广域网信息安全管理工作具有重要意义。

教学重点

- 广域网可能面临的信息安全风险。
- 防火墙在广域网中的应用。
- VPN 技术在广域网中的应用。
- 基于广域网的电子商务安全。
- 基于广域网的电子政务安全。

7.1　广域网的风险

21 世纪全世界的计算机都将通过 Internet 连到一起，随着 Internet 的发展，网络丰富的信息资源给用户带来了极大的方便，但同时也给上网用户带来了安全问题。由于 Internet 的开放性和超越组织与国界等特点，使它在安全性上存在一些隐患。而且信息安全的内涵也发生了根本的变化。它不仅从一般性的防卫变成了一种非常普通的防范，而且还从一种专门的领域变成了无处不在。

1．网络入侵/攻击（包括木马）

Internet 是一个开放的、无控制机构的网络，黑客（Hacker）经常会侵入网络中的计算机系统，或窃取机密数据和盗用特权，或破坏重要数据，或使系统功能得不到充分发挥直至瘫痪。

2．网络病毒

计算机病毒通过 Internet 的传播给上网用户带来极大的危害，病毒可以使计算机和计算机网络系统瘫痪、数据和文件丢失。在网络上传播病毒可以通过公共匿名 FTP 文件传送、也可以通过邮件和邮件的附加文件传播。

3．隐私泄露

上网账号、QQ 密码、游戏账号、银行账号、邮件密码、个人隐私及其他重要个人信息的泄露都会给自己带来不同程度的损失和不便，正是这样的原因，阻碍了一部分人不敢放心地使用网络。

4．网上收费陷阱

网上收费陷阱就是通过一些不实宣传或者误导性手段，通常采用的手法就是以提供免费服务为名义，诱导用户申请某些自己并不需要的网络服务，然后向客户收取费用。

5．网上虚假信息

网民上网的一个主要目的就是获取信息，以满足自己的应用需要，如果网上存在虚假信息，那么必将给网民带来损失，必然的结果就是导致人们失去对网络信息的信任，最后影响网络的健康发展。

6．垃圾邮件

垃圾邮件多数是广告信息，还有部分是以传播病毒、木马程序等为目的，垃圾邮件至少有三大直接危害。

（1）占用大量传输、存储和运算资源，造成邮件服务器拥堵，降低了网络的运行效率，严重影响正常的邮件服务；

（2）垃圾邮件以其数量多、反复性、强制性、欺骗性、不健康性和传播速度快等特点，严重干扰用户的正常生活，侵犯收件人的隐私权和信箱空间，并耗费收件人的时间、精力、金钱。

（3）妖言惑众、骗人钱财、传播色情、反动等内容的垃圾邮件，已经对现实社会造成危害。

7．诱骗/欺诈/网络钓鱼

网络钓鱼(phishing)是在网络上盗窃身份的一种形式。它使用诱骗性的电子邮件和欺骗性质的网站来引诱人们泄露信用卡号、注册用户名、密码和社会保障号码等个人财务信息，盗取用户资金。一般情况下，不法分子利用欺骗性的电子邮件和伪造的网页，骗取银行客户输入个人账户资料、密码等，并利用骗子取得用户卡号和密码，制作成假的银行卡，在 ATM 上取钱或进行网上支付等活动，使用户蒙受经济损失。

7.2　防火墙技术应用

防火墙作为网络安全体系结构中基础的信息安全设备，在与 Internet 的网络中，起着安全防范作用。

7.2.1　防火墙部署

防火墙作为一种保护内部网络免受攻击的重要安全技术，需要部署在内部网络和外部网络的边界处。根据具体的网络结构不同，部署方式有所区别，下面介绍防火墙在几种常见的网络结构中的部署情况。

1．普通企业环境

这是最为普通的企业环境防火墙部署案例。利用防火墙将网络分为三个安全区域，企业内部网络，外部网络和服务器专网(DMZ 区)。内部网络一般采用私有的 IP 地址，DMZ 的服务器可以采用公网地址，也可以采用私有地址，但是需要在防火墙上做相应的地址转换来保证外部用户对服务器的正常访问。一般常用的安全策略是：外部网络不允许访问内部网络，内部网络用户可以根据不同的权限访问 Internet 资源；内部用户和外部用户只允许访问 DMZ 区指定服务器的指定服务。具体的环境如图 7-1 所示。

2．ADSL 接入的部署

ADSL 接入是一种经济实惠的 Internet 接入方式，防火墙提供了对 ADSL 接入，也就是 PPPOE 拨号的支持。用防火墙代替原有的拨号客户端来连接 ADSL Modem，实现自动拨号的功能，可以配置防火墙自动做一条动态的地址转换，实现内部的多个用户通过一条 ADSL 实现对互联网的访问。这样防火墙配置的一般策略为只允许内部网络访问外部网络的指定服务。具体的环境如图 7-2 所示。

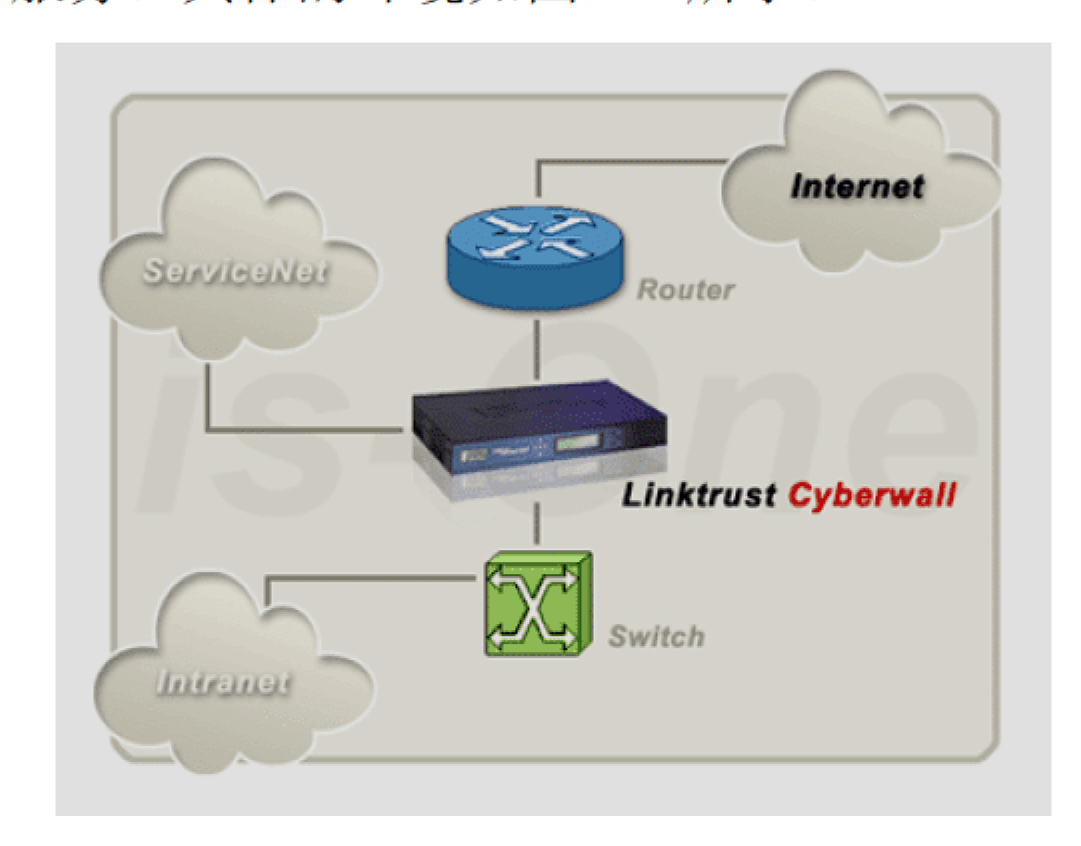


图 7-1 普通企业防火墙部署

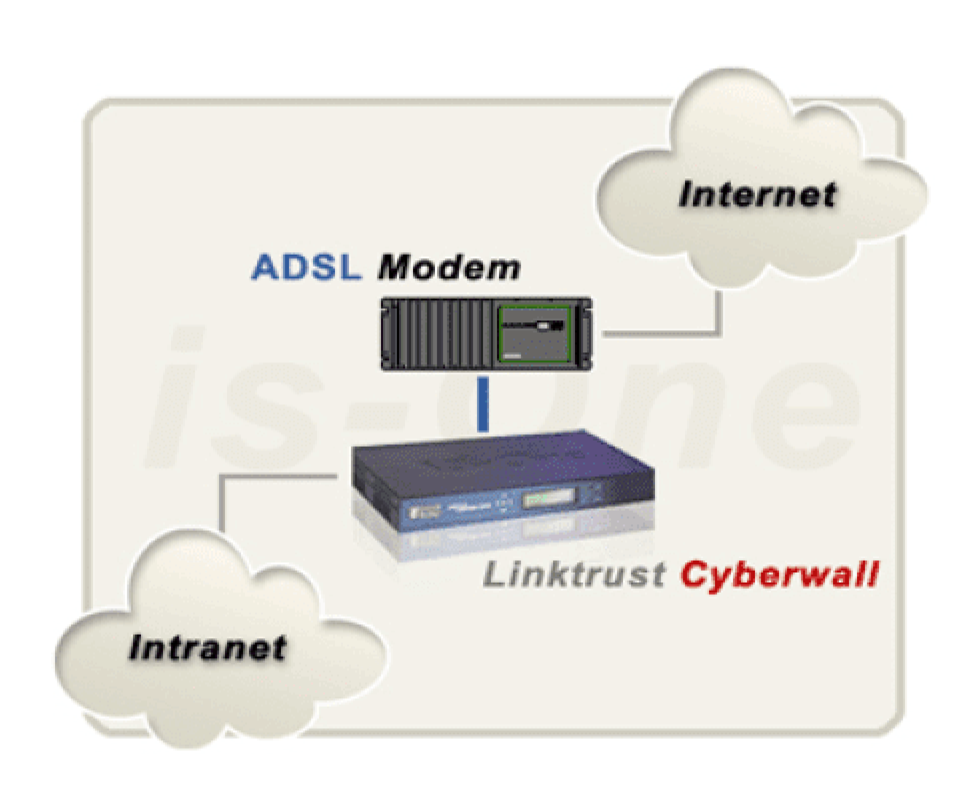


图 7-2 防火墙代替 ADSL 接入部署

3．网络多出口部署

经常会碰到企业的局域网有多个出口，比如 Internet 出口，总部出口等。防火墙支持将 DMZ 接口作为一个外网接口，支持多出口的接入。例如我们可以将防火墙的外网口 Internet 接入服务器，将 DMZ 口接入总部接入的服务器，如图 7-3 所示，利用路由的选择来分流去往两个区域的流量，可以将默认的网关指向 Internet 处的路由器，添加相应的去往总部网络方向的路由策略。然后针对不同的网络之间的数据通信，采用相应的安全策略。另外的一种多出口的接入方式也可以用两个防火墙的方式，分别对应于相应的链路，如图 7-4 所示，这种方式也可以利用路由的选择来实现。

单台防火墙实现多出口的接入如图 7-3 所示。

两台防火墙实现多出口的接入如图 7-4 所示。

4．高可靠性配置的部署

高可靠性网络的部署是为了避免因为网络的故障和设备的停工造成的损失。防火墙支持全面的高可靠性解决方案，包括防火墙之间的冗余配置和整体链路的冗余配置。配置防火墙冗余总共需要三套 IP 地址，其中每个防火墙有一套自己真实的地址（内部地址，外部地址和 DMZ 区地址），另外两个防火墙还共享一套虚拟的地址，而真正起作用的正是这

套真实的地址，内部用户的网关以及外部的一些相关的路由设置都需要指向这个虚拟的地址。防火墙的心跳传输也非常灵活，可以采用单独的网口进行心跳，也可以采用某一条网络连接。防火墙本身的冗余配置具体的环境如图 7-5 所示。

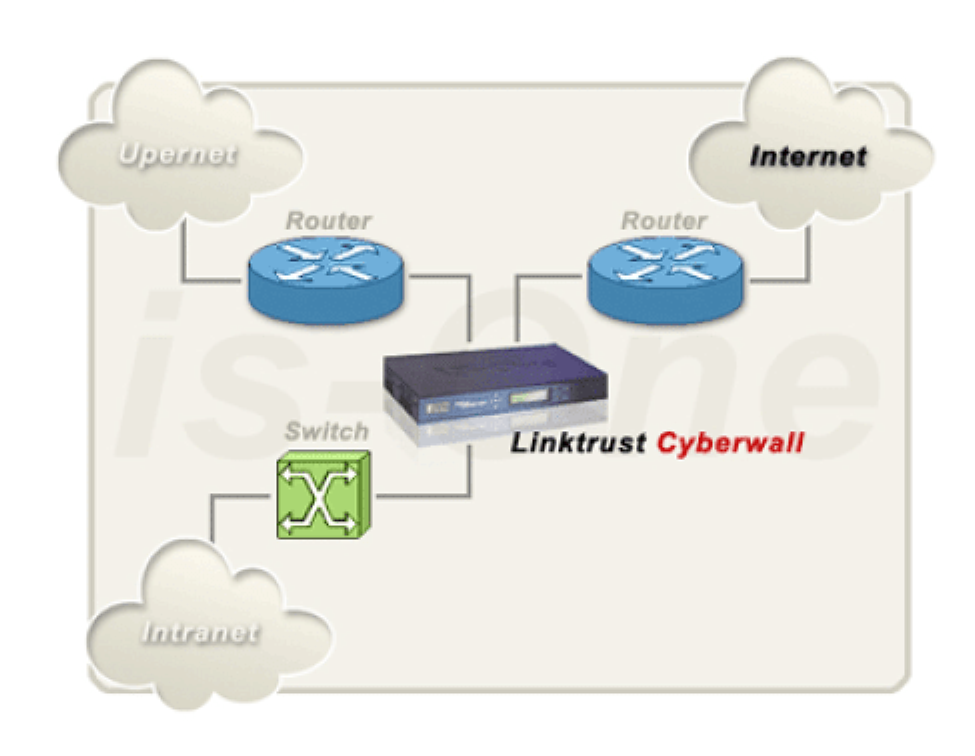


图 7-3　单台防火墙实现多出口的接入

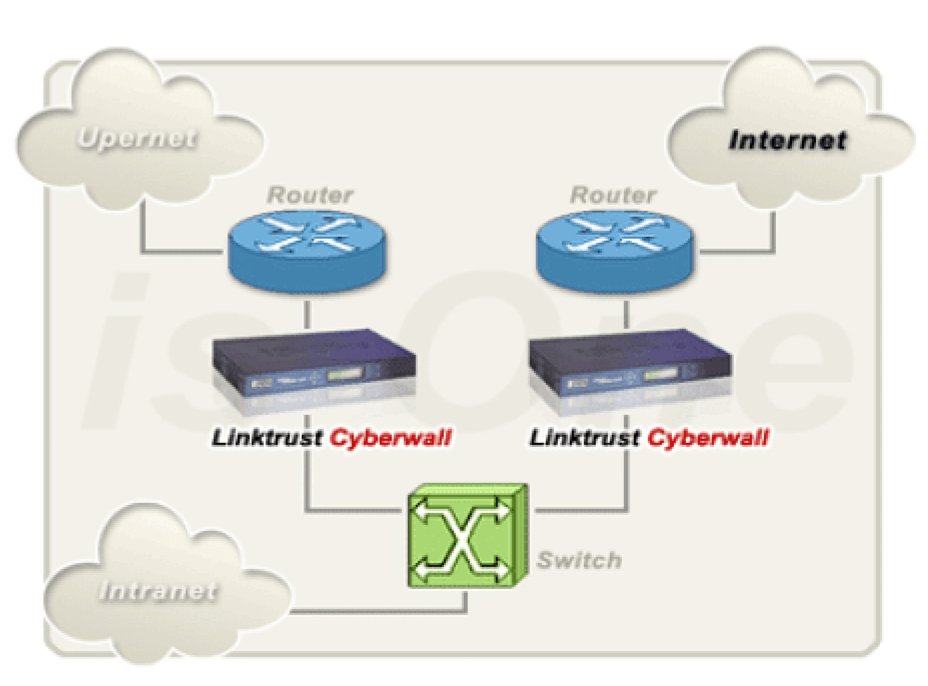


图 7-4　两台防火墙实现多出口的接入

整体链路的冗余配置如图 7-6 所示。

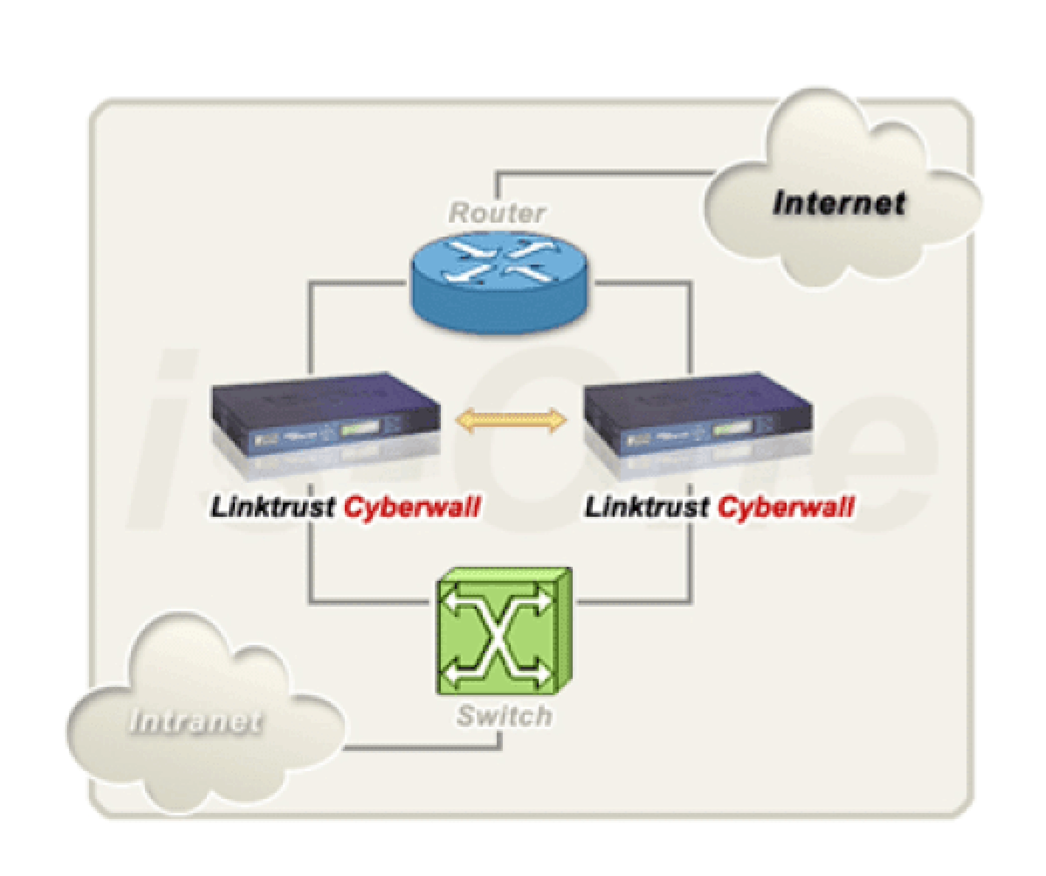


图 7-5　防火墙本身的冗余配置

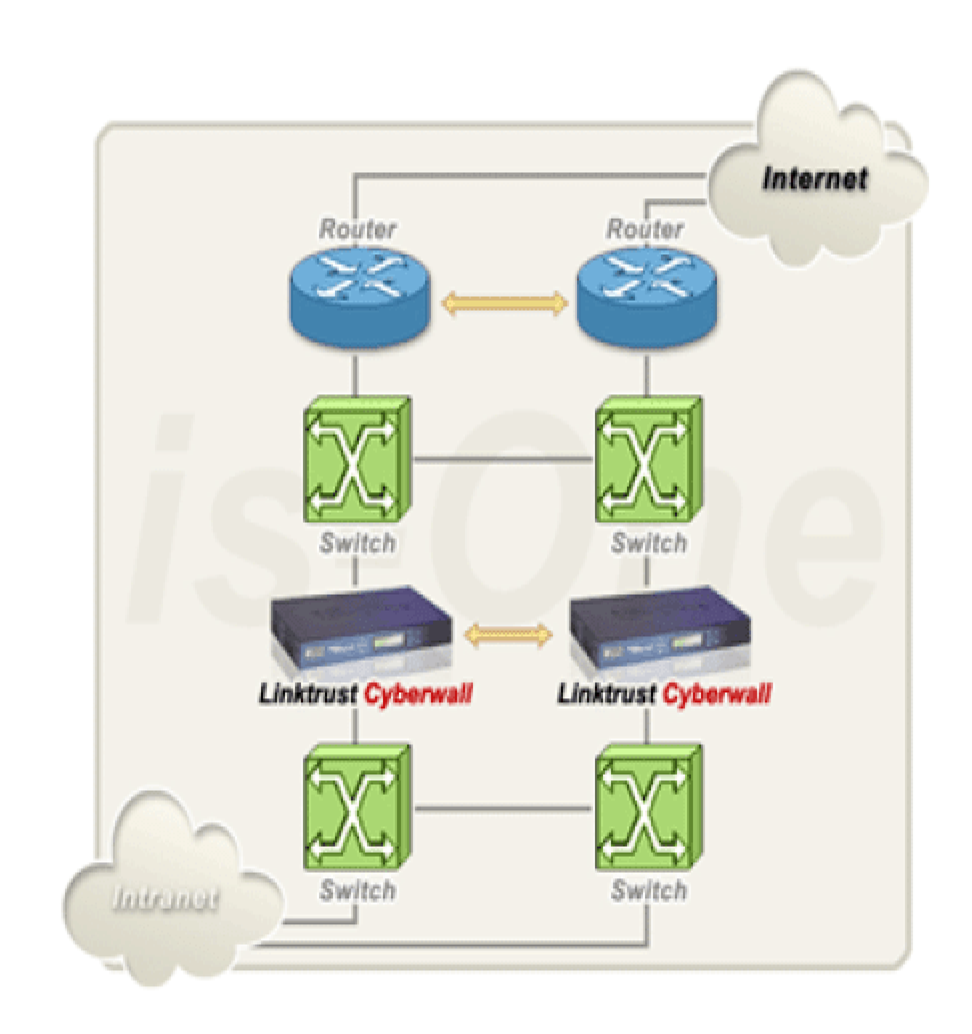


图 7-6　整体链路的冗余配置

5. 分布式网络环境的部署

分布式的环境一般分为一个中心节点和多个分支节点，防火墙支持对这种结构的整体配置。一般来说，中心节点采用性能高的防火墙，可以采用双机热备份的模式，保证网络的可靠性；对于较大的有专线接入的分支节点，可以采用防火墙，一方面保证该分支网络的边界安全，另外也可以通过 VPN 功能实现与总部的信息通信的安全；对于没有专线的分支节点，可以采用防火墙自带的对子网拨号的 VPN 功能，也能够实现与总部之间的安全通信。如图 7-7 所示。

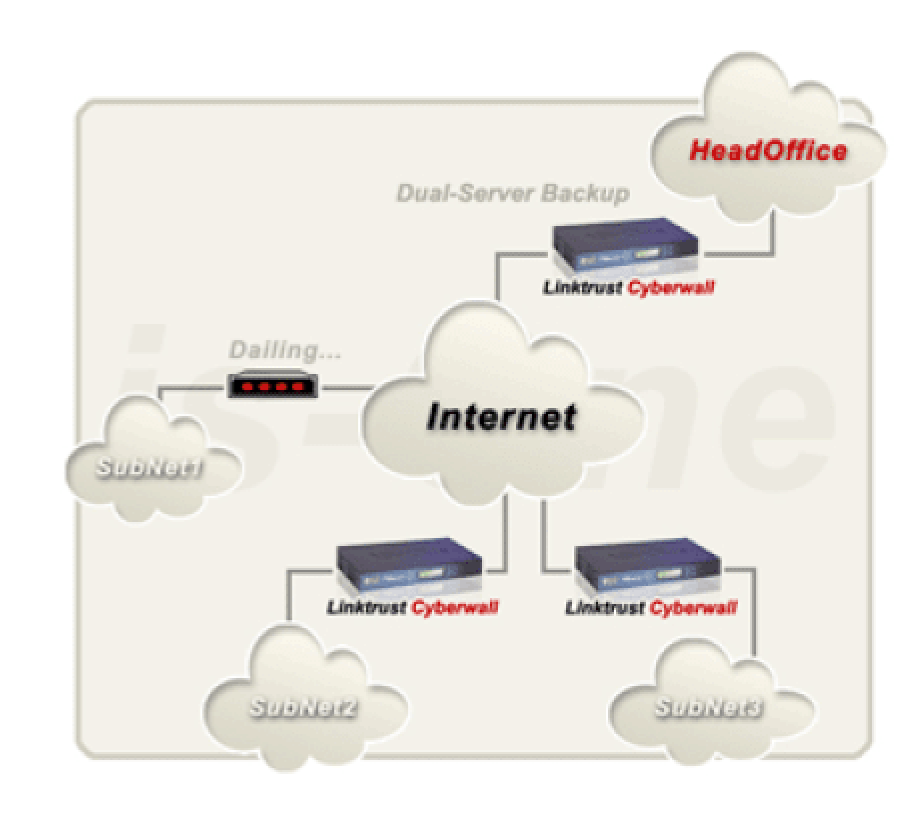


图 7-7　分布式网络环境的部署

7.2.2 防火墙的配置

防火墙的具体配置方法并没有统一的标准，这与具体的产品有关，主要原因体现在三个方面：（1）不同厂商的防火墙产品具有不同的配置风格；（2）相同厂商生产的不同用途的防火墙其配置方法不同；（3）相同厂商的同类防火墙不同版本的配置方法有所改变。在此以 CISCO 公司出品的 PIX 系列防火墙的配置为例介绍一些基本的配置原则。

1．配置前的准备工作

CISCO 公司开发的 PIX 防火墙系列设备，主要起到策略过滤，隔离内外网，根据用户实际需求设置 DMZ（隔离区）。它和一般硬件防火墙一样具有转发数据包速度快，可设定的规则种类多，配置灵活的特点。图 7-8 为 CISCO 的一款产品的外观。

PIX 防火墙从外观上和路由器差不多。如图 7-8 所示，正面没有任何接口，只显示指示灯。所有的接口都在 PIX 防火墙的背面，如图 7-9 所示。



图 7-8 防火墙产品的外观

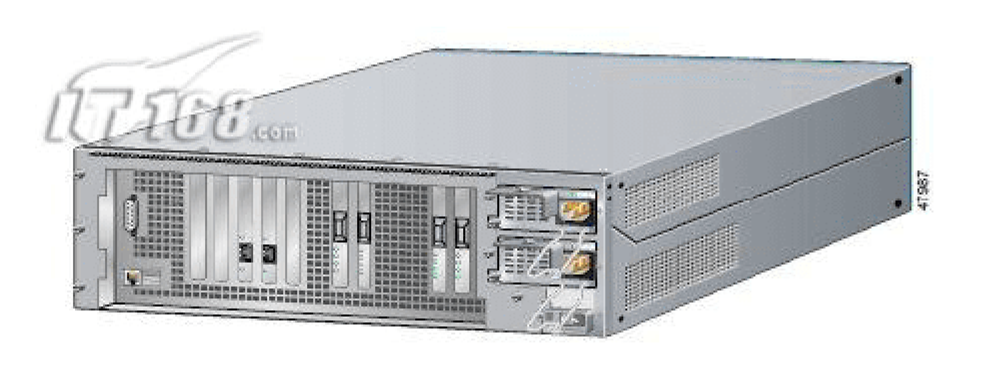


图 7-9 防火墙的背面接口

发现该设备接口很多，从 RJ45 到 USB 接口，从显示器接口到电源接口。我们进一步放大背面各个接口可以看得更加清晰。如图 7-10 所示。

可以根据图中的指示找到对应的接口，当然默认情况下只有这些接口，如果我们希望添加某个类型的接口还可以卸下相应的面板自行安装新接口。我们用到最多的是 CONSOLE 口（控制台）和 Slot5，Slot6（RJ45 网线接口）。

安装 PIX 和安装普通的路由器和交换机一样，用螺丝将设备固定在机柜上即可，同时注意散热和 UPS 不间断电源的供应。

一台新的 PIX 防火墙不经过任何配置是无法投入使用的。我们需要用 CONSOLE 线连接设备的 CONSOLE 接口并根据实际应用环境进行设置，登录 PIX 的管理界面很简单，将 CONSOLE 线连接控制台接口即可。如图 7-11 所示。

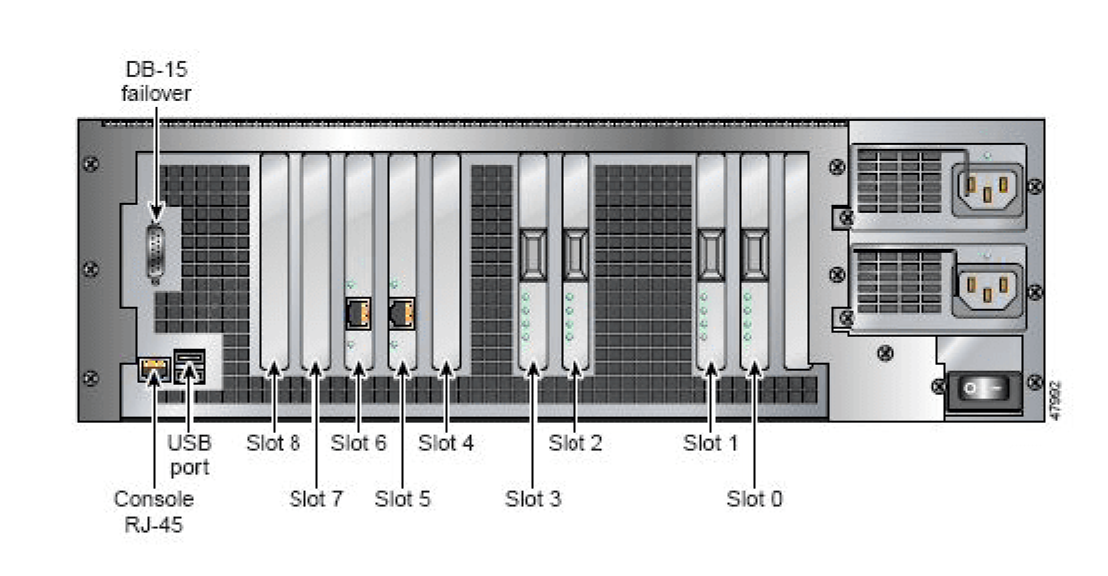


图 7-10 放大后的防火墙背面

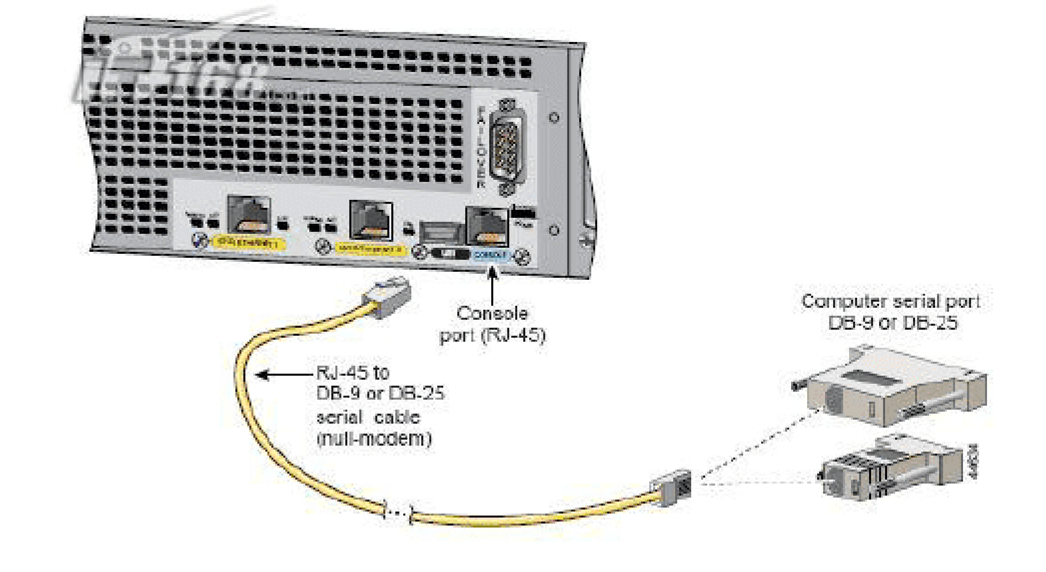


图 7-11 防火墙控制接口

在配置 PIX 防火墙之前，首先了解一下防火墙的物理特性。防火墙通常具有至少 3 个接口，但许多早期的防火墙只具有 2 个接口；当使用具有 3 个接口的防火墙时，就至少产生了三个网络，三个网络的基本描述如下。

（1）内部区域（内网），内部区域通常就是指企业内部网络或者是企业内部网络的一部分。它是互连网络的信任区域，即受到了防火墙的保护。

（2）外部区域（外网），外部区域通常指 Internet 或者非企业内部网络。它是互连网络中不被信任的区域，当外部区域想要访问内部区域的主机和服务，通过防火墙，就可以实现有限制的访问。

（3）隔离区（DMZ），隔离区是一个隔离的网络或几个网络。位于隔离区中的主机或服务器被称为堡垒主机。一般在隔离区内可以放置 Web 服务器、Mail 服务器等。隔离区对于外部用户通常是可以访问的，这种方式让外部用户可以访问企业的公开信息，但却不允许他们访问企业内部网络。

提示： DMZ 是英文 demilitarized zone 的缩写，中文名称为“隔离区”，也称“非军事化区”。早期的防火墙功能很有限，只有两个接口，因此这类防火墙是没有隔离区的。

了解了 PIX 的区域划分后我们还需对防火墙的管理访问模式有所区分。实际上 PIX 防火墙和 CISCO 以往的路由交换设备一样有四个管理访问模式。依次如下。

（1）非特权模式。PIX 防火墙开机自检后，就是处于这种模式。系统显示 pixfirewall>提示符。

（2）特权模式。在非特权模式下输入 enable 进入特权模式，可以改变当前配置。显示 pixfirewall#提示符。

（3）配置模式。在特权模式下输入 configure terminal 进入此模式，绝大部分的系统配置都在这里进行。显示 pixfirewall(config)#提示符。

（4）监视模式。PIX 防火墙在开机或重启过程中，按住 Escape 键或发送一个 Break 字符，进入监视模式。这里可以更新操作系统映像和口令恢复。显示 monitor>提示符。

这四个管理访问模式我们最常用的还是特权模式和配置模式，95%以上的操作命令都是在这两个模式下完成的，而监视模式主要用于恢复 PIX 默认密码等调试工作，非特权模式则只能查看 PIX 设备运行状况，不能修改任何设置。

2. 防火墙的基本配置原则

默认情况下，所有的防火墙都是按以下两种情况配置的。

（1）拒绝所有的流量，这需要在你的网络中特殊指定能够进入和出去的流量的一些类型。

（2）允许所有的流量，这种情况需要你特殊指定要拒绝的流量的类型。

通常情况下，大多数防火墙默认都是拒绝所有的流量作为安全选项。一旦安装防火墙后，需要打开一些必要的端口来使防火墙内的用户在通过验证之后可以访问系统。换句话说，如果想让员工们能够发送和接收 E-mail，必须在防火墙上设置相应的规则或开启允许 POP3 和 SMTP 的进程。

在防火墙的配置中，首先要遵循的原则就是安全实用，从这个角度考虑，在防火墙的配置过程中需坚持以下三个基本原则。

（1）简单实用：对防火墙环境设计来讲，首要的就是越简单越好。其实这也是任何事物的基本原则。越简单的实现方式，越容易理解和使用。而且是设计越简单，越不容易出

错，防火墙的安全功能越容易得到保证，管理也越可靠和简便。

每种产品在开发前都会有其主要功能定位，比如防火墙产品的初衷就是实现网络之间的安全控制，入侵检测产品主要针对网络非法行为进行监控。但是随着技术的成熟和发展，这些产品在原来的主要功能之外或多或少地增加了一些增值功能，比如在防火墙上增加了查杀病毒、入侵检测等功能，在入侵检测上增加了病毒查杀功能。但是这些增值功能并不是所有应用环境都需要，在配置时我们也可针对具体应用环境进行配置，不必要对每一功能都详细配置，这样一则会大大增强配置难度，同时还可能因各方面配置不协调，引起新的安全漏洞，得不偿失。

（2）全面深入：单一的防御措施是难以保障系统的安全的，只有采用全面的、多层次的深层防御战略体系才能实现系统的真正安全。在防火墙配置中，不要停留在几个表面的防火墙语句上，而应系统地看待整个网络的安全防护体系，尽量使各方面的配置相互加强，从深层次上防护整个系统。这方面可以体现在两个方面：一方面体现在防火墙系统的部署上，多层次的防火墙部署体系，即采用集互联网边界防火墙、部门边界防火墙和主机防火墙于一体的层次防御；另一方面将入侵检测、网络加密、病毒查杀等多种安全措施结合在一起的多层安全体系。

（3）内外兼顾：防火墙的一个特点是防外不防内，其实在现实的网络环境中，80%以上的威胁都来自内部，所以我们要树立防内的观念，从根本上改变过去那种防外不防内的传统观念。对内部威胁可以采取其他安全措施，比如入侵检测、主机防护、漏洞扫描、病毒查杀。这方面体现在防火墙配置方面就是要引入全面防护的观念，最好能部署与上述内部防护手段一起联动的机制。

3．防火墙的初始配置

在使用之前，防火墙需要经过基本的初始配置，才能使防火墙发挥作用，下面我们对这一过程做一个简单的介绍。

防火墙的初始配置也是通过控制端口（Console）与 PC（通常是便于移动的笔记本电脑）的串口连接，再通过 Windows 系统自带的超级终端（HyperTerminal）程序进行选项配置。防火墙的初始配置物理连接参见图 7-11 所示。

防火墙除了以上所说的通过控制端口（Console）进行初始配置外，也可以通过 telnet 和 Tffp 配置方式进行高级配置，但 Telnet 配置方式都是在命令方式中配置，难度较大，而 Tffp 方式需要专用的 Tffp 服务器软件，但配置界面比较友好。

防火墙的具体配置步骤如下。

（1）将防火墙的 Console 端口用一条防火墙自带的串行电缆连接到笔记本电脑的一个空余串口上，如图 7-11 所示。

（2）打开 PIX 防火墙电源，让系统加电初始化，然后开启与防火墙连接的主机。

（3）运行计算机 Windows 系统中的超级终端（HyperTerminal）程序（通常在“附件”程序组中）。

（4）当 PIX 防火墙进入系统后即显示 pixfirewall>的提示符，这就证明防火墙已启动成功，所进入的是防火墙用户模式。可以进行进一步的配置了。

（5）输入命令：enable，进入特权用户模式，此时系统提示为 pixfirewall#。

（6）输入命令：configure terminal，进入全局配置模式，对系统进行初始化设置。

① 首先配置防火墙的网卡参数（以只有 1 个 LAN 和 1 个 WAN 接口的防火墙配置为例）。

命令为：Interface ethernet0 auto

#0 网卡系统自动分配为 WAN 网卡，auto 选项为系统自适应网卡类型

② 配置防火墙内、外部网卡的 IP 地址

命令格式为：IP address inside ip_address netmask

Inside 代表内部网卡

命令格式为：IP address outside ip_address netmask

outside 代表外部网卡

③ 指定外部网卡的 IP 地址范围：

命令格式为：global 1 ip_address-ip_address

④ 指定要进行转换的内部地址

命令格式为：nat 1 ip_address netmask

⑤ 配置某些控制选项：

命令格式为：conduit global_ip port[-port] protocol foreign_ip [netmask]

其中，global_ip：指的是要控制的地址；port：指的是所作用的端口，0 代表所有端口；protocol：指的是连接协议，比如：TCP、UDP 等；foreign_ip：表示可访问的 global_ip 外部 IP 地址；netmask：为可选项，代表要控制的子网掩码。

（7）配置保存

命令格式为：wr mem

（8）退出当前模式

此命令为 exit，可以任何用户模式下执行，执行的方法也相当简单，只输入命令本身即可。它与 Quit 命令一样。下面三条语句表示了用户从配置模式退到特权模式，再退到普通模式下的操作步骤。

pixfirewall(config)# exit

pixfirewall# exit

pixfirewall>

（9）查看当前用户模式下的所有可用命令：show，在相应用户模式下输入这个命令后，即显示出当前所有可用的命令及简单功能描述。

（10）查看端口状态：show interface，这个命令需在特权用户模式下执行，执行后即显示出防火墙所有接口配置情况。

（11）查看静态地址映射：show static，这个命令也须在特权用户模式下执行，执行后显示防火墙的当前静态地址映射情况。

7.3　VPN 技术

实现跨区域局域网之间互相通信的最有效方式就是使用 VPN，具有的最大特点是在不需要增加通信线路的情况下实现安全传输。

7.3.1 VPN 基础

1. 远程访问

远程访问是指通过透明的方式将位于本地网络以外（远程网络）位置上的特定计算机连接到本地网络中的一系列相关技术。当启用远程访问时，远程客户可以通过远程访问技术像直接连接到本地网络一样来使用本地网络中的资源。在 Windows 服务器操作系统中均包含了远程访问服务，它是作为路由和远程访问服务中的一个组件，远程访问服务支持远程访问客户端使用拨号网络连接和虚拟专用网络连接这两种方式的远程访问。

（1）拨号网络连接远程访问方式：通过拨号远程访问方式，远程访问客户端可以利用电信基础设施（通常情况下为模拟电话线路）来创建通向远程访问服务器的临时物理电路或虚拟电路。一旦这种物理电路或虚拟电路被创建，其余连接参数将通过协商方式加以确定。

（2）虚拟专用网络（VPN）连接远程访问方式：通过虚拟专用网络远程访问方式，VPN 客户端可以通过 IP 网络（例如 Internet）与充当 VPN 服务器的远程访问服务器建立虚拟点对点连接。一旦这种虚拟点对点连接被创建，其余连接参数将通过协商方式加以确定。

由于 IP 网络的流行，拨号网络连接远程访问方式已经基本不再使用。在此仅对虚拟专用网络（VPN）连接远程访问方式进行阐述。对于一个完整的 VPN 远程访问连接，它由以下元素组成。

（1）远程访问 VPN 客户端

VPN 客户端既可以是独立的计算机，也可以是建立站点到站点 VPN 连接的 VPN 服务器。而根据 VPN 客户端类型的不同，VPN 分为以下两种连接类型。

① 远程访问 VPN：由一台独立的计算机作为 VPN 客户端向 VPN 服务器发起 VPN 连接，从而此 VPN 客户端计算机可以访问 VPN 服务器所连接的内部网络中的资源。Windows XP、Windows 2000、Windows NT 4.0、Windows ME 和 Windows 98 VPN 客户端均可与 Windows 的 VPN 服务器或运行其他大多数 VPN 服务器的远程访问服务器建立 VPN 连接。这种类型的 VPN 又称为客户端到服务器 VPN。

② 站点到站点 VPN：在连接到不同内部网络的两台 VPN 服务器之间进行 VPN 连接，当 VPN 连接成功建立后，它们所连接的内部网络中均可以相互进行访问，就像直接通过物理链路连接到一起。VPN 服务器会将通过 VPN 连接的数据进行加密和封装，但是本地子网中的客户和 VPN 服务器之间的通信并不会进行加密。Windows 的 VPN 服务器均可以和其他 VPN 服务器创建站点到站点的 VPN 连接。这种类型的 VPN 又称为网关 VPN 或路由器到路由器 VPN。

（2）远程访问 VPN 服务器

基于 Windows 服务器操作系统的远程访问服务器能够接受基于 PPTP 或 L2TP/IPSec 的远程访问 VPN 连接，或者基于 PPTP、L2TP/IPSec 或 IPSec 隧道模式的站点到站点 VPN 连接。

远程访问 VPN 客户端必须能够通过 IP 网络访问到远程访问 VPN 服务器，如果 VPN 服务器位于某个内部网络而 VPN 客户端位于 Internet 之上，那么必须在 VPN 服务器连接到 Internet 的网关上为 VPN 服务器做端口映射。

（3）VPN 协议

Windows 远程访问服务器与客户端支持两种远程访问 VPN 协议。

- 点对点隧道协议（PPTP）
- 第二层隧道协议（L2TP）

而对于站点到站点 VPN 连接，除了使用上述协议外，你还可以使用 IPSec 隧道模式。

1）点对点隧道协议（PPTP）

点对点隧道协议（PPTP）是微软基于 PPP 协议开发的隧道协议，在 RFC 2637 中进行定义，在 Windows 系统中广泛使用。PPTP 首先在 Windows NT 4.0 中提供支持，并且随 TCP/IP 协议一起自动进行安装。PPTP 是点对点协议（PPP）的一种扩展，它采用了 PPP 所提供的身份验证、压缩与加密机制，并且通过 Microsoft 点对点加密（MPPE）技术来对数据包进行加密、封装和隧道传输。

PPTP 具有以下特性：

① PPTP 帧通过通用路由封装（Generic Routing Encapsulation，GRE，协议 ID 47）报头和 IP 报头（TCP 1723）进行封装，在 IP 报头中提供了与 VPN 客户端和 VPN 服务器相对应的源 IP 地址和目标 IP 地址；

② 使用 Microsoft 点对点加密（MPPE）技术来对多种协议的数据包进行加密、封装和在 IP 网络上进行隧道传输；

③ PPTP 隧道连接协商身份验证、压缩与加密；

④ PPTP 支持 VPN 客户端 IP 地址的动态分配；

⑤ MPPE 使用 RSA/RC4 算法和 40 位、56 位或 128 位的密钥进行加密；

⑥ MPPE 将通过由 MS-CHAP、MS-CHAP v2 或 EAP-TLS 身份验证过程所生成的加密密钥对 PPP 帧进行加密，因此为对 PPP 帧中所包含的有效数据进行加密，虚拟专用网络客户端必须使用 MS-CHAP、MS-CHAP v2 或 EAP-TLS 身份验证协议；PPTP 将利用底层 PPP 加密功能并直接对原先经过加密的 PPP 帧进行封装；

⑦ 初始加密密钥在用户身份验证时产生并且定期刷新；

⑧ 在 PPTP 数据包中，只有数据负载才进行了加密。

如果使用 PPTP 协议的 VPN 客户端部署在 NAT 网关之后，那么要求 NAT 网关具有理解 PPTP 协议的 NAT 编辑器，否则 VPN 客户将不能创建 VPN 连接。目前的绝大部分 NAT 网关中都具有 PPTP NAT 编辑器，均可以很好地支持 PPTP 协议。

2）第二层隧道协议（L2TP）

第二层隧道协议（L2TP）是微软 PPTP 隧道协议和 CISCO 第二层转发协议（L2F）的结合体，在 RFC 2661 中进行定义（最新的版本是 L2TPv3，在 RFC 3931 中定义）。与 PPTP 利用 MPPE 进行数据包加密不同，L2TP 依靠 Internet 协议安全性（IPSec）技术提供加密服务。L2TP 与 IPSec 的结合产物称为 L2TP/IPSec，VPN 客户端与 VPN 服务器都必须支持 L2TP 和 IPSec 才能使用 L2TP/IPSec。L2TP 将随同路由与远程访问服务一起自动进行安装。

在 IPSec 数据包基础上所进行的 L2TP 封装由两个层次组成：

L2TP 封装： PPP 帧（IP 或 IPX 数据包）将通过 L2TP 报头和 UDP 报头进行封装。

IPSec 封装：上述封装后所得到的 L2TP 报文将通过 IPSec 封装安全性有效载荷（ESP）报头、用以提供消息完整性与身份验证的 IPSec 身份验证报尾以及 IP 报头再次进行封装。

IP 报头中将提供与 VPN 客户端和 VPN 服务器相对应的源 IP 地址和目标 IP 地址。IPSec 加密机制将通过由 IPSec 身份验证过程所生成的加密密钥对 L2TP 报文进行加密。

L2TP 具有以下特性：

① L2TP 隧道数据可以在任何支持点对点传输的网络中进行传输，例如 IP、帧中继、ATM 网络等等；

② L2TP 使用 UDP 协议来进行隧道管理；

③ L2TP 基于 UDP 协议发送封装的 PPP 数据包；

④ 负载数据可以被加密和压缩；

⑤ 使用 IPSec 封装安全性有效载荷（ESP）进行加密，IPSec ESP 在 RFC 3193 中进行定义；

⑥ 虽然 L2TP/IPSec 提供了用户验证机制，但是同样要求计算机进行验证。计算机验证是相互的，每一端的计算机都必须向对方进行验证；

⑦ 对于计算机验证，要求计算机证书。VPN 客户端和 VPN 服务器（远程访问 VPN），或两端的 VPN 服务器（站点到站点 VPN）都必须具有有效的证书。你可以配置使用预共享的 L2TP 密钥，这样就无需计算机证书，但是由于所有 VPN 客户都必须配置相同的预共享密钥，这样带来的后果是极大地降低了 L2TP 的安全性。

⑧ 每一端都必须能够验证另一端提供的证书是否有效，如果计算机证书是由不同的证书权威颁发，那么会出现问题。

和 PPTP 协议不一样，如果基于 L2TP/IPSec 协议的 VPN 客户端部署在 NAT 网关之后，只有 VPN 服务器和 VPN 客户端支持 IPSec NAT 穿越(NAT-T)时，VPN 客户端才能和 VPN 服务器成功创建 VPN 连接。NAT-T 在 RFC 3947 中进行定义，它描述了 IPSec 协议如何穿越 NAT 服务器。和 L2TP/IPSec 使用 UDP 端口 500、1701 不同，NAT-T 使用 UDP 4500 端口。Windows Server 2003、Microsoft L2TP/IPSec VPN 客户端软件和 L2TP/IPSec NAT-T 更新后的 Windows XP 和 Windows 2000 支持 NAT-T。

但是，微软不推荐在 NAT 网关后的 Windows Server 2003 上使用 IPSec NAT-T，并且修改了 Windows XP SP2 中的 IPSec 通信行为，使其默认情况下不再支持 NAT 网关后的 IPSec NAT-T。

（4）IPSec 隧道模式

对于站点到站点 VPN 连接，除了上述的 PPTP 和 L2TP/IPSec 外，你还可以使用 IPSec 隧道模式。IPSec 隧道模式单独使用 IPSec 来创建一个加密的隧道，通常用于和不支持 L2TP/IPSec 或 PPTP 协议的非 Windows VPN 服务器之间创建加密通信。和 L2TP、PPTP 不同，IPSec 隧道模式不需要验证用户账户，它具有以下特性：

① IP 数据包通过 IPSec 进行加密，并在 IP 网络上进行隧道传输；

② IPSec 隧道模式只能用于站点到站点的 VPN 类型；

③ IPSec 隧道模式需要额外的 IPSec 安全策略配置；

2．选择远程访问 VPN 协议

PPTP 和 L2TP/IPSec 的区别主要有：

① PPTP 使用 MPPE 进行加密，L2TP/IPSec 和 IPSec 隧道模式使用 IPSec ESP 进行加密。

② PPTP 加密在 PPP 身份验证通过后处理连接时开始，因此，身份验证过程没有被 MPPE 加密。L2TP/IPSec 会先进行安全协商再进行身份验证，并对 PPP 身份验证数据包进行加密，因此 L2TP/IPSec 比 PPTP 提供了更高的安全性。

③ PPTP 使用 MMPE 和 RC4，而 L2TP/IPSec 使用 DES 或 3DES。

④ PPTP 和 L2TP/IPSec 均要求用户使用基于 PPP 的身份验证协议进行身份验证。

⑤ L2TP/IPSec 还要求使用计算机证书进行计算机验证。因此，L2TP/IPSec 提供了更强壮的身份验证过程。但是，带来的不便之处是 L2TP/IPSec 需要公共密钥基础服务（PKI）或预共享的连接密钥，而 PPTP 则无需 PKI。

⑥ IPSec ESP 要求基于数据包的数据源验证和数据完整性验证，另外，IPSec ESP 提供了中继保护，这防止了数据包的重现攻击；而 PPTP 没有提供这些保护。

⑦ IPSec ESP 和 PPTP（通过使用 MPPE）提供了基于每个数据包的加密。

⑧ 你可以将基于 PPTP 的 VPN 服务器部署在 NAT 网关后，但是不建议将基于 L2TP/IPSec、IPSec 的 VPN 服务器部署在 NAT 网关后。

⑨ L2TP/IPSec 比 PPTP 更耗费 CPU 性能。

在选择 VPN 协议时，你应考虑以下几点：

① 是否存在公共密钥基础服务（PKI），如果不存在则选择 PPTP；强烈建议不要在商用网络中通过预共享的连接密钥来使用 L2TP，这样会极大地降低 L2TP 的安全性；

② 如果要求最高的安全级别，选择 L2TP/IPSec；

③ 只有在特别需要时才使用 IPSec 隧道模式；

④ 如果企业安全策略要求 DES 或 3DES，则使用 L2TP/IPSec；

⑤ 如果使用 IPSec 导致 CPU 负荷过重，使用 PPTP；

⑥ 如果 VPN 服务器部署在 NAT 网关后，选择 PPTP；

⑦ 部署 PPTP 比部署 IPSec 更为简单。

对于 VPN 客户的身份验证、访问授权和记账，你可以选择两种不同的方式：Windows 或 RADIUS。你可以为这三种功能选择一种方式，也可以选择一种方式用于身份验证和授权，而另一种用于记账。

当使用 Windows 验证时，如果 VPN 服务器是独立服务器，则使用本地账户（SAM）来验证 VPN 客户；如果 VPN 服务器是域成员服务器，则使用活动目录数据库来验证 VPN 客户。如果使用 RADIUS 进行身份验证，那么就算 VPN 服务器是独立服务器，也可以通过 RADIUS 使用活动目录数据库来进行验证。在 Windows 服务器中同样提供了 RADIUS 服务器组件，不过被称为 Internet 验证服务器（IAS）。

PPTP 和 L2TP/IPSec 均要求用户进行身份验证，并且对于 L2TP/IPSec，你必须配置用户身份验证和计算机身份验证。Windows VPN 服务器支持的身份验证方式有：

① 可扩展身份验证协议（EAP）；

② Microsoft 质询式握手身份验证协议（MS-CHAP）；

③ MS-CHAP 第 2 版（MS-CHAP v2）；

④ 质询式握手身份验证协议（CHAP）；

⑤ Shiva 式口令身份验证协议（SPAP）；

⑥ 可扩展身份验证协议（EAP，包含 EAP-MD5、EAP-TLS、EAP/MS-CHAPv2 等等）。

它们之间的详细区别请参考 Windows 的帮助，常用的身份验证方式是 MS-CHAP、MS-CHAP v2 和 EAP-TLS。

如果此 RRAS 服务器属于活动目录，你需要提升域功能级为 Windows 2000 Native 或者 Windows Server 2003 后，才能使用通过远程访问策略控制访问选项。并且此 RRAS 服务器的计算机账户必须加入到域本地安全组 RAS and IAS Servers 组中，否则该 RRAS 服务器不能读取域用户的拨入权限设置。在启用路由和远程访问服务时，会自动加入到 RAS and IAS Servers 组中，如果没有自动加入，你可以手动进行添加或者在路由和远程访问服务器上运行 Netsh ras add registeredserver 命令。

当 VPN 服务器允许 VPN 客户拨入 VPN 时，将会为 VPN 客户分配一个 IP 地址。你可以配置 VPN 服务器通过内部网络中的 DHCP 服务器来为 VPN 客户分配一个 IP 地址，也可以手动配置一个静态 IP 地址范围来为 VPN 客户进行分配。但是，如果配置使用和内部网络不一致的子网来用于 VPN 客户的地址分配时，你必须添加内部网络通过 VPN 服务器到达 VPN 客户的路由。

当 VPN 客户创建 VPN 拨号连接时，默认会启用远程网络上的默认网关，即把 VPN 连接作为自己的默认网关。这将导致 VPN 客户不能访问除自己本地子网外的其他本地网络，也不能通过本地网络连接到 Internet。

7.3.2 部署 VPN

远程访问 VPN 是一台独立的 VPN 客户计算机向 VPN 服务器发起的 VPN 连接，Windows 的远程访问 VPN 服务是作为路由和远程访问（RRAS）服务的一个组件来提供，它支持 PPTP 或者 L2TP/IPSec 协议的 VPN 连接。在 Windows Server 2003 中部署远程访问 VPN 服务，从而支持 VPN 客户端使用 PPTP 和 L2TP/IPSec 协议进行远程访问 VPN 连接。

其实 VPN 部署比较简单，你只需要考虑以下几点。

① 决定身份验证方式（Windows 还是 RADIUS）。在此将使用 Windows 来进行身份验证。

② 身份验证方法。在此将使用默认的 MS-CHAP、MS-CHAP v2 和 EAP-TLS。

③ 用户拨入授权方式（显式允许访问还是通过远程访问策略授权）。在此将显式允许用户远程拨入访问。

④ VPN 客户地址分配方式（使用内部网络中的 DHCP 服务或者使用静态 IP 地址范围）。在此试验中由于内部网络中没有 DHCP 服务，所以将采用静态 IP 地址范围 172.16.0.1～172.16.0.254。

⑤ 对于 L2TP/IPSec，还需要部署证书服务。在此试验中内部网络中已经部署了证书权威服务器。

试验环境如图 7-12 所示，Internet 上的 VPN 客户端 Perth（IP 地址为 61.139.0.8）将通过 Munich（外部 IP 地址为 61.139.0.1，内部 IP 地址为 10.1.1.1）上的 VPN 服务连接到内部网络（10.1.1.0/24）中。Milan 是内部网络上的 Web 服务器和证书服务器，IP 地址为 10.1.1.9。所有计算机的操作系统均为 Windows Server 2003 SP1，并且均为独立服务器，在进行试验之前已经确保网络连接工作正常。

试验步骤如下。

（1）在 VPN 服务器上启用路由和远程访问服务中的远程访问 VPN 服务；

（2）VPN 服务器上显式允许用户 Administrator 的远程拨入；

（3）在 VPN 客户端上创建 PPTP 模式的 VPN 连接并进行测试。

1. 启用路由和 VPN 服务

（1）在 VPN 服务器上以管理员身份登录，选择“开始”|“程序”|“管理工具”|“路由和远程访问”命令，出现“路由和远程访问”窗口，如图 7-13 所示。

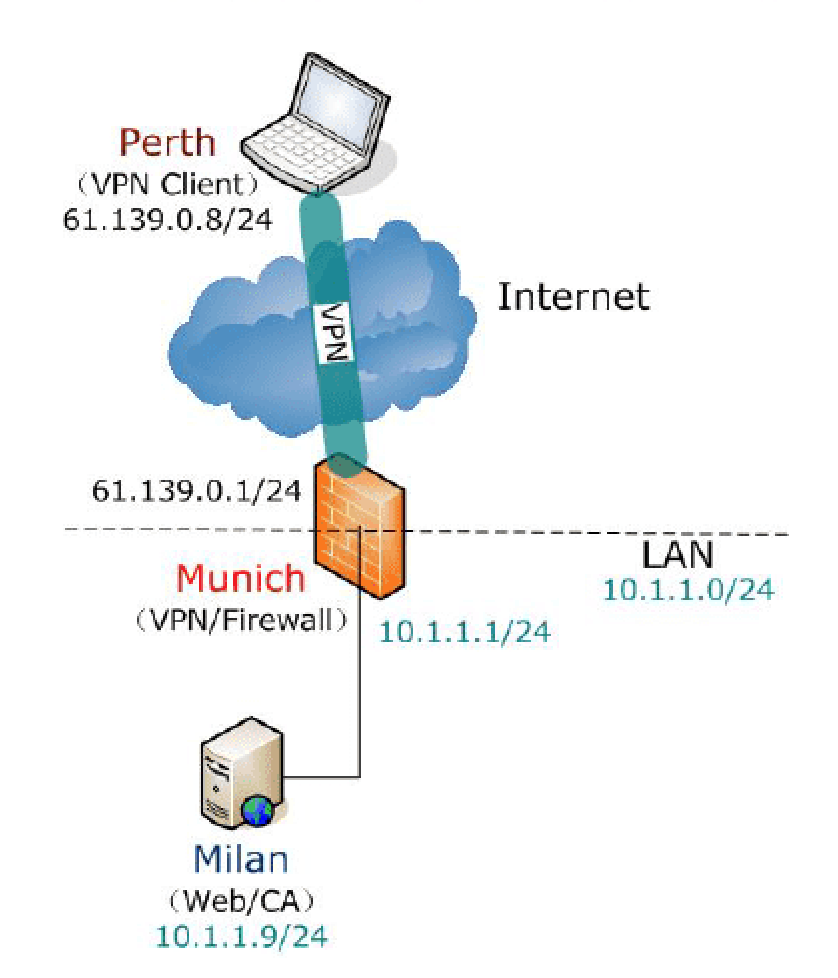


图 7-12　试验环境示意图

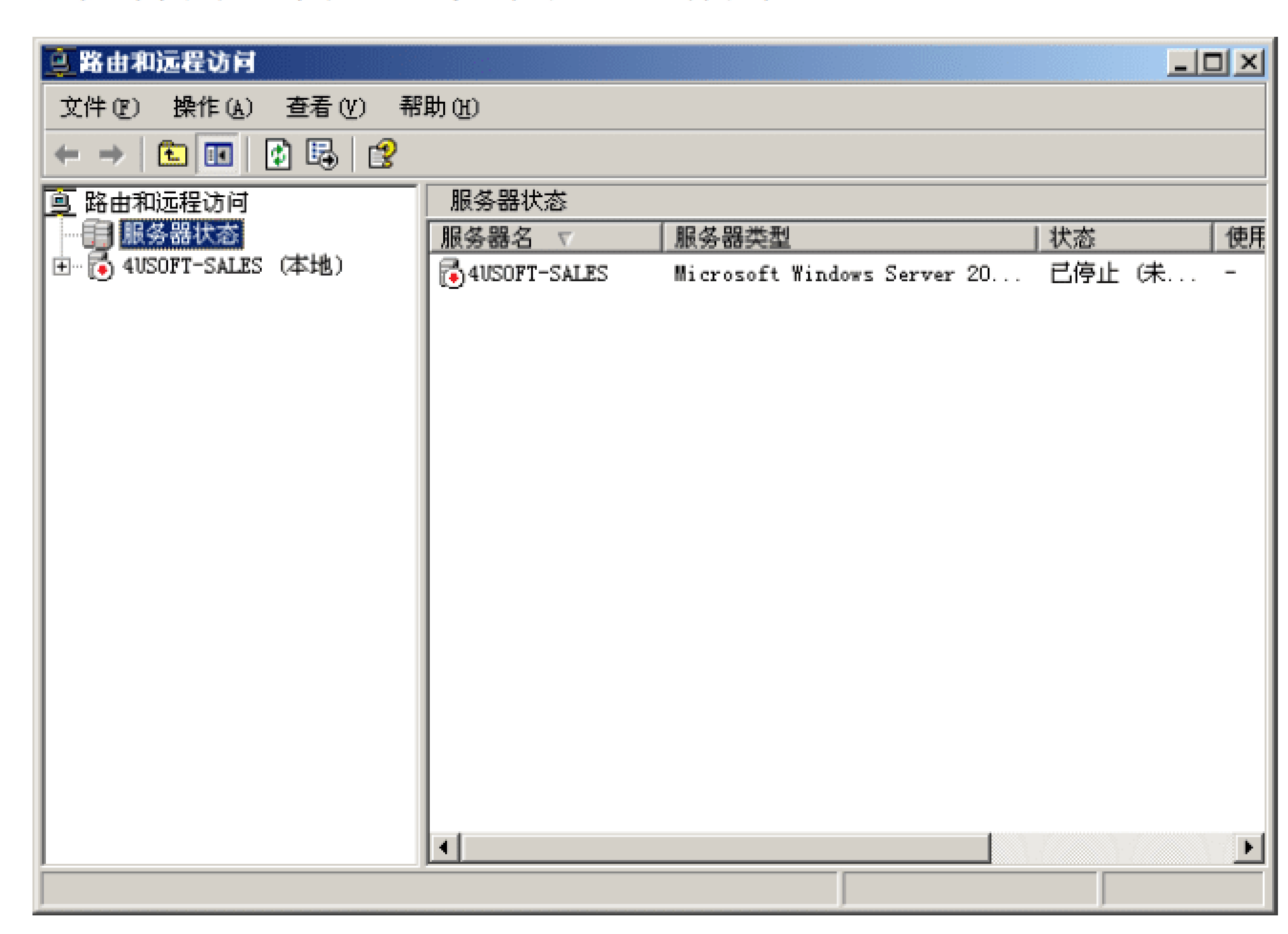


图 7-13　路由和远程访问

（2）在“路由和远程访问”窗口中，右击 4usoft-sales 服务器，在菜单中选择“配置并启用路由和远程访问”命令，出现“路由和远程访问服务器安装向导”欢迎对话框，单击“下一步”按钮，出现如图 7-14 对话框。

（3）选择“自定义配置”单选框，然后单击“下一步”按钮，出现如图 7-15 所示对话框。

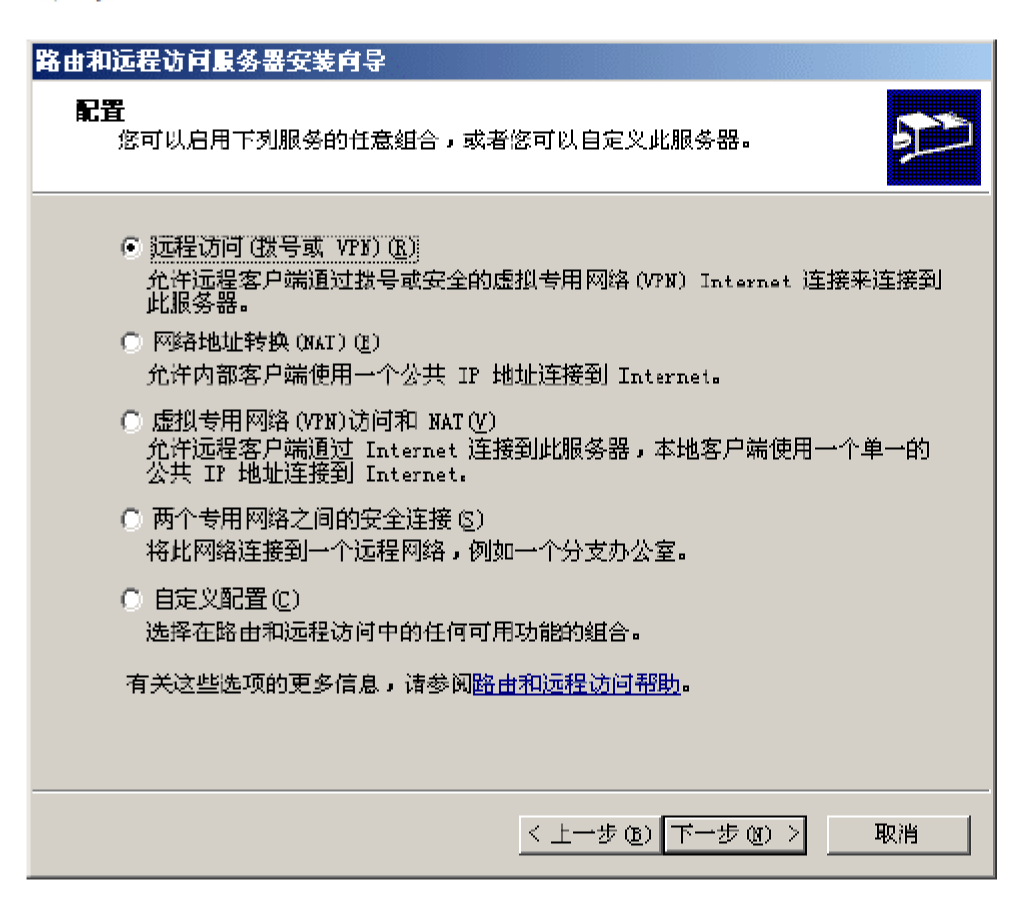


图 7-14　路由和远程访问配置

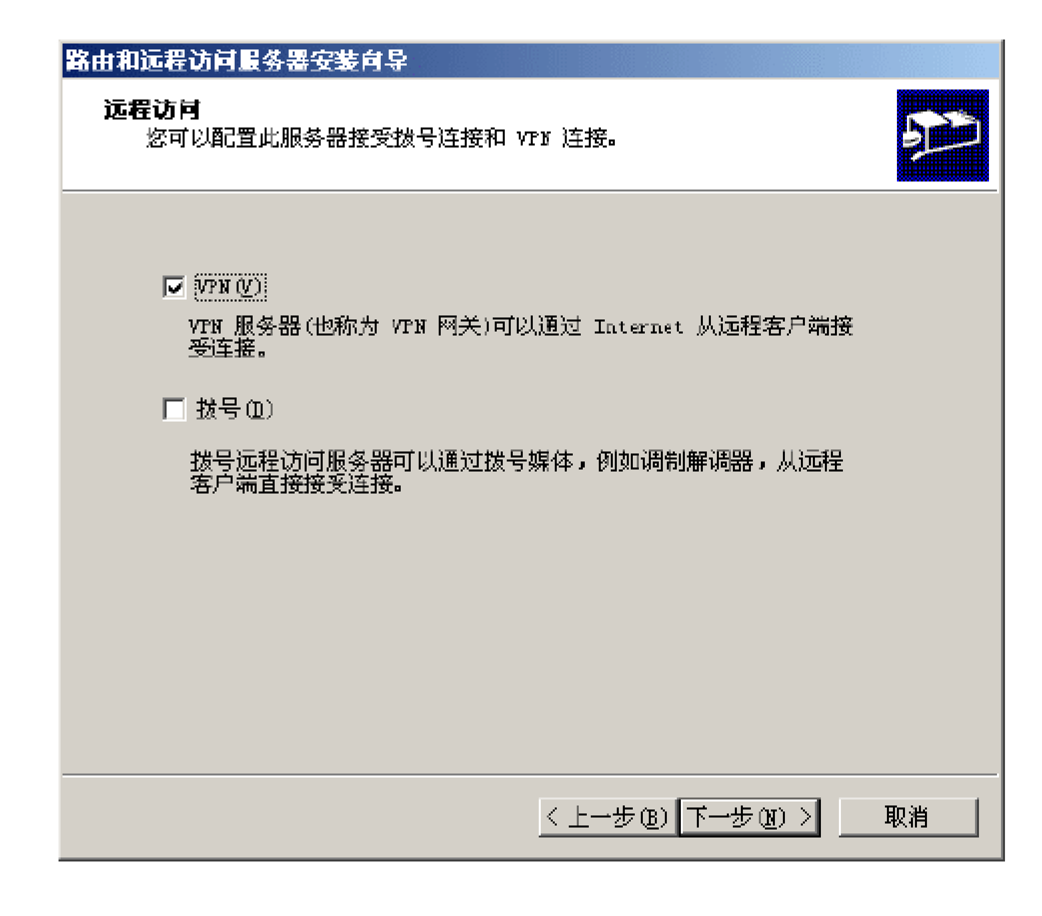


图 7-15　远程访问配置

（4）在“远程访问”配置窗口中，选择 VPN 复选框，单击“下一步”按钮，如图 7-16 所示。

（5）单击“下一步”按钮，出现完成配置提示对话框，如图 7-17 所示。

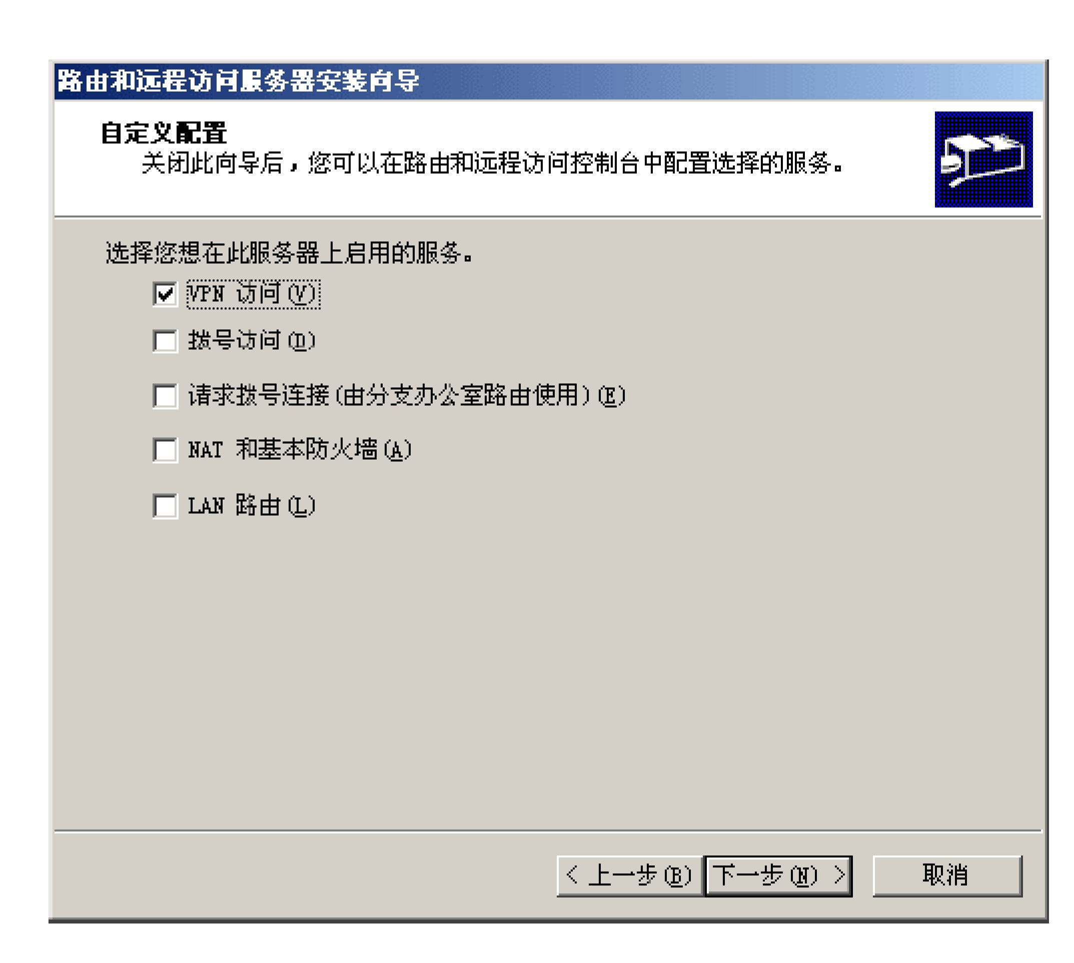


图 7-16 自定义配置窗口

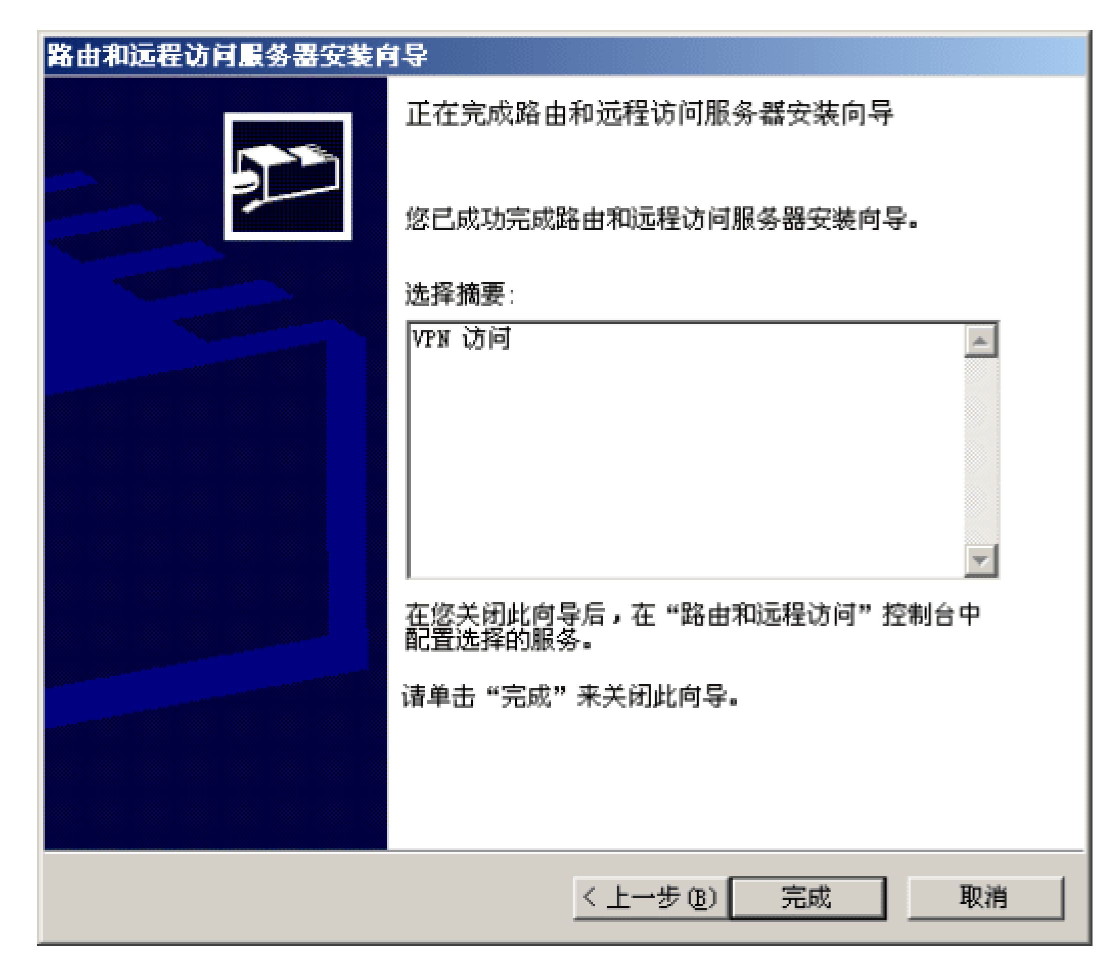


图 7-17 完成配置窗口

（6）单击“完成”按钮，完成“路由和远程访问”的配置，系统出现提示对话框，提示是否现在启动服务，选择“是”按钮，现在启动“路由和远程访问”服务，如图 7-18 所示。

（7）在“路由和远程访问”窗口中右击“端口”，在弹出菜单中选择“属性”，出现“端口 属性” 对话框，如图 7-19 所示。

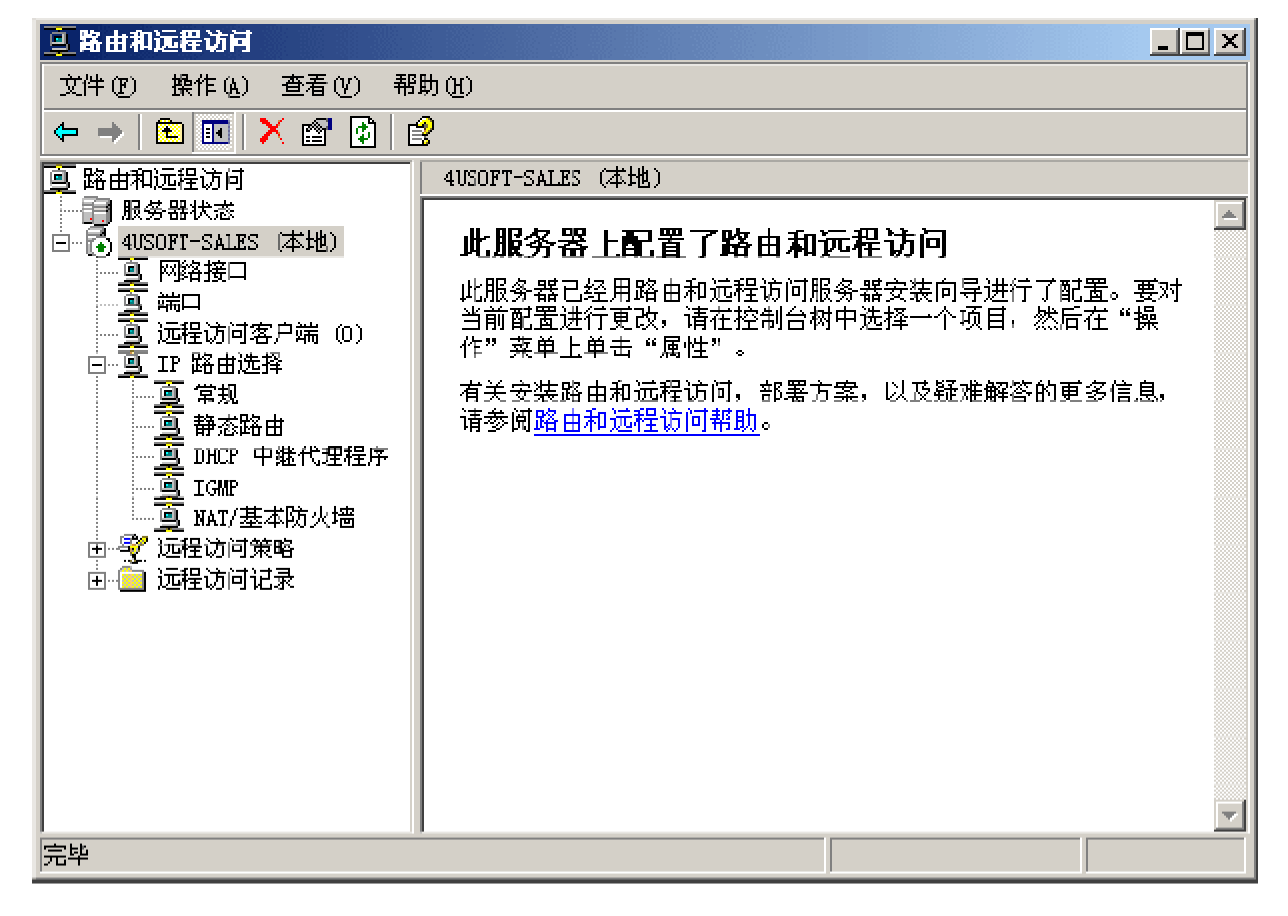


图 7-18 配置完成并启动的路由和远程访问

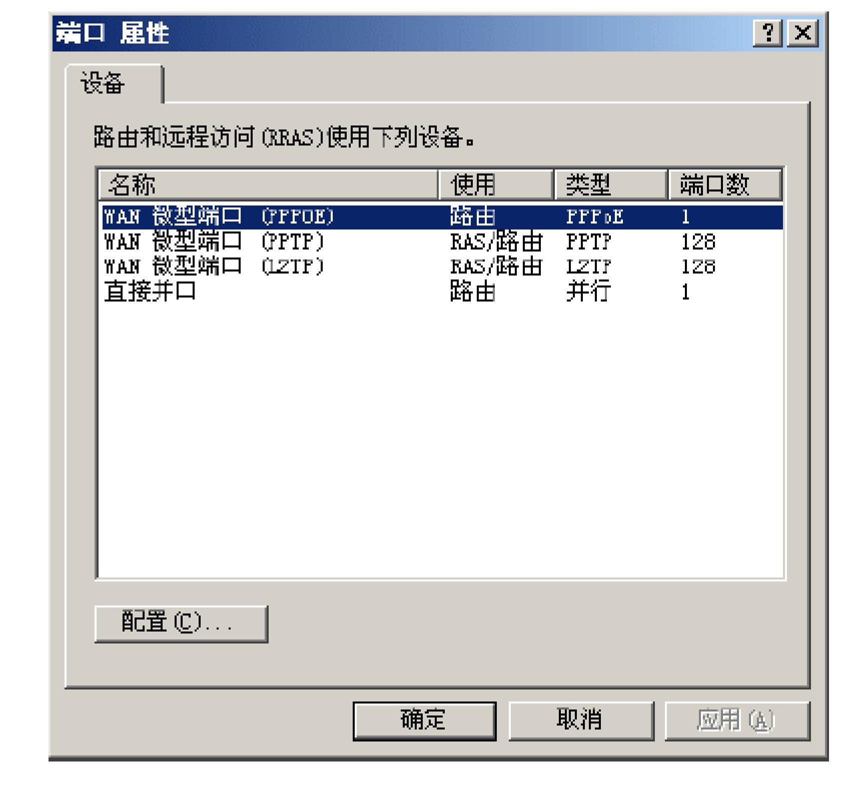


图 7-19 端口属性

（8）在“端口 属性”对话框中，选择端口后单击“配置”按钮，出现配置窗口，如图 7-20 所示。

（9）在配置设备对话框中修改最多端口数为需要的数量，这里保持默认设置为 128。

2．允许用户 Administrator 的远程拨入

（1）选择“开始”|“程序”|“管理工具”|“计算机管理”命令，出现“计算机管理”窗口，如图 7-21 所示。

（2）选择“计算机管理（本地）”|“系统工具”|“本地用户和组”|“用户”，双击右边的 Administrator 用户名，出现“Administrator 属性”对话框，并选择“拨入”选项卡，如图 7-22 所示。

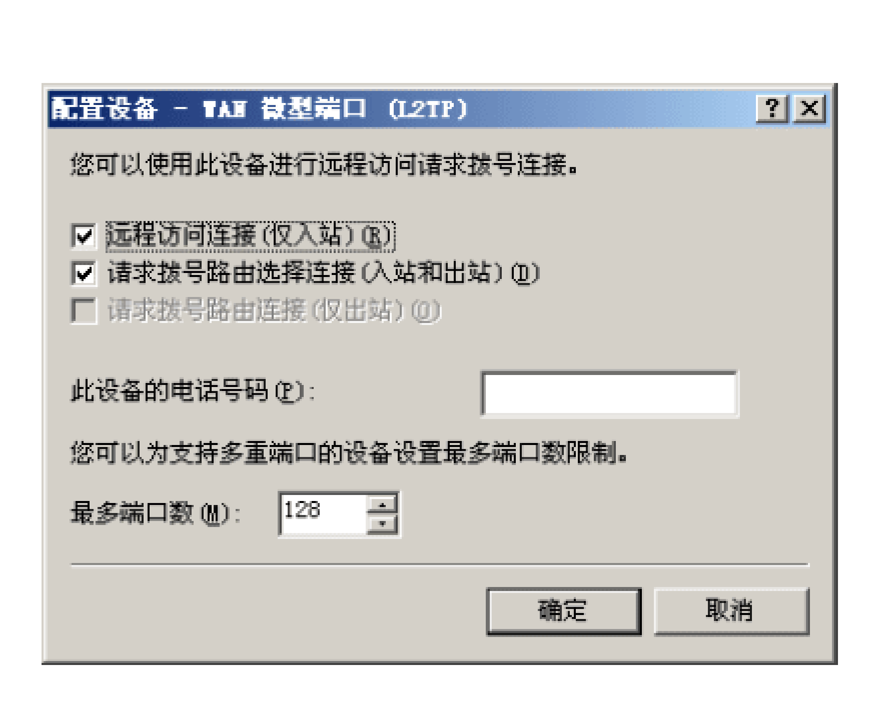


图 7-20　配置设备对话框

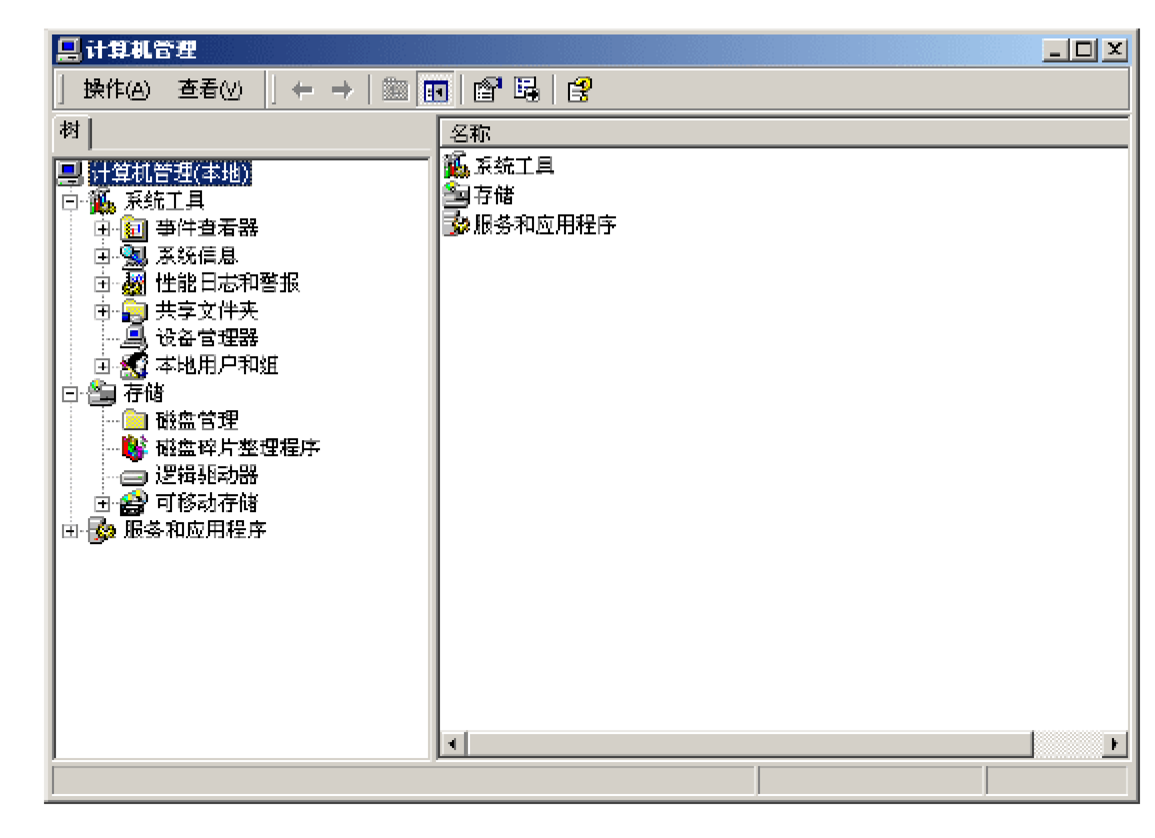


图 7-21　计算机管理窗口

（3）在“远程访问权限（拨入或 VPN）”选项区域中选择“允许访问”单选框，单击“确定”按钮，这样就完成允许 Administrator 用户拨入 VPN 了。

3．在 VPN 客户端创建 PPTP 模式的 VPN 连接

（1）在 VPN 客户端上以管理员身份登录，选择“开始”|“设置”|“网络连接”|“新建连接向导”命令，出现“新建连接向导”窗口，如图 7-23 所示。

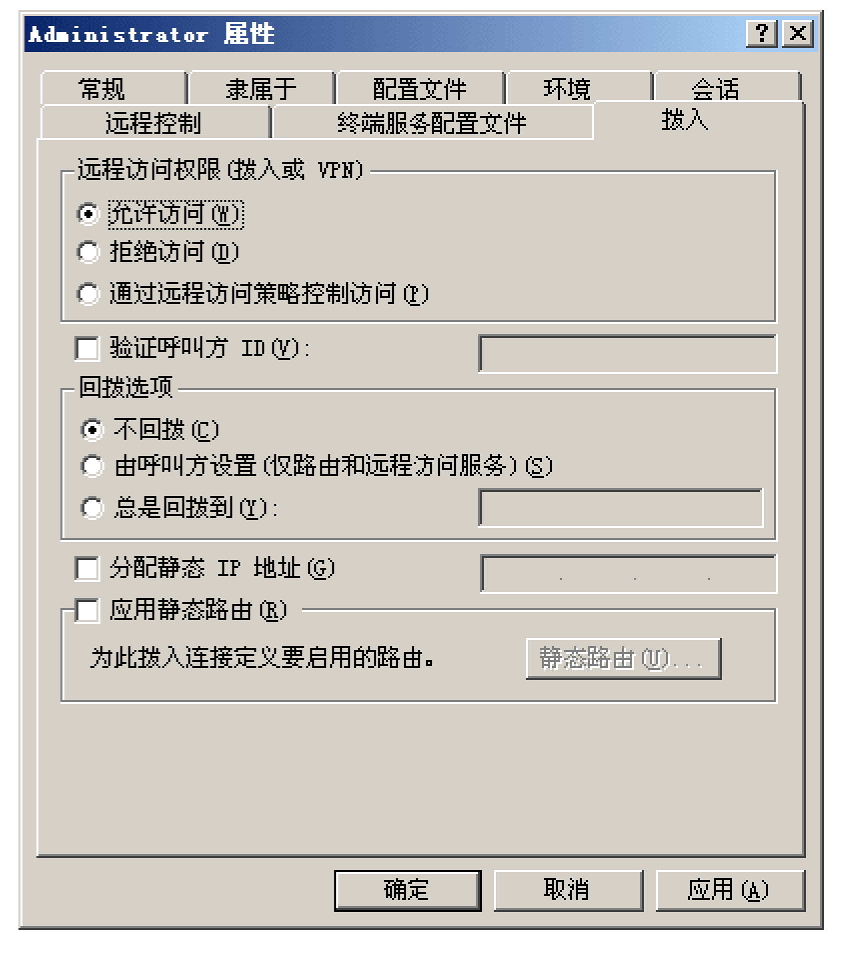


图 7-22　用户属性对话框



图 7-23　新建连接向导欢迎窗口

（2）在“新建连接向导”窗口中单击“下一步”按钮，出现网络连接类型设置窗口，如图 7-24 所示。

（3）选择“连接到我的工作场所的网络”单选框，单击“下一步”按钮，出现选择连接方式对话框，如图 7-25 所示。

（4）选择“虚拟专用网络连接”单选框，单击“下一步”按钮，出现设置连接名称对话框，如图 7-26 所示。

（5）设置完成公司名后，单击“下一步”按钮，出现设置 VPN 服务器名或者 IP 地址的对话框，如图 7-27 所示。

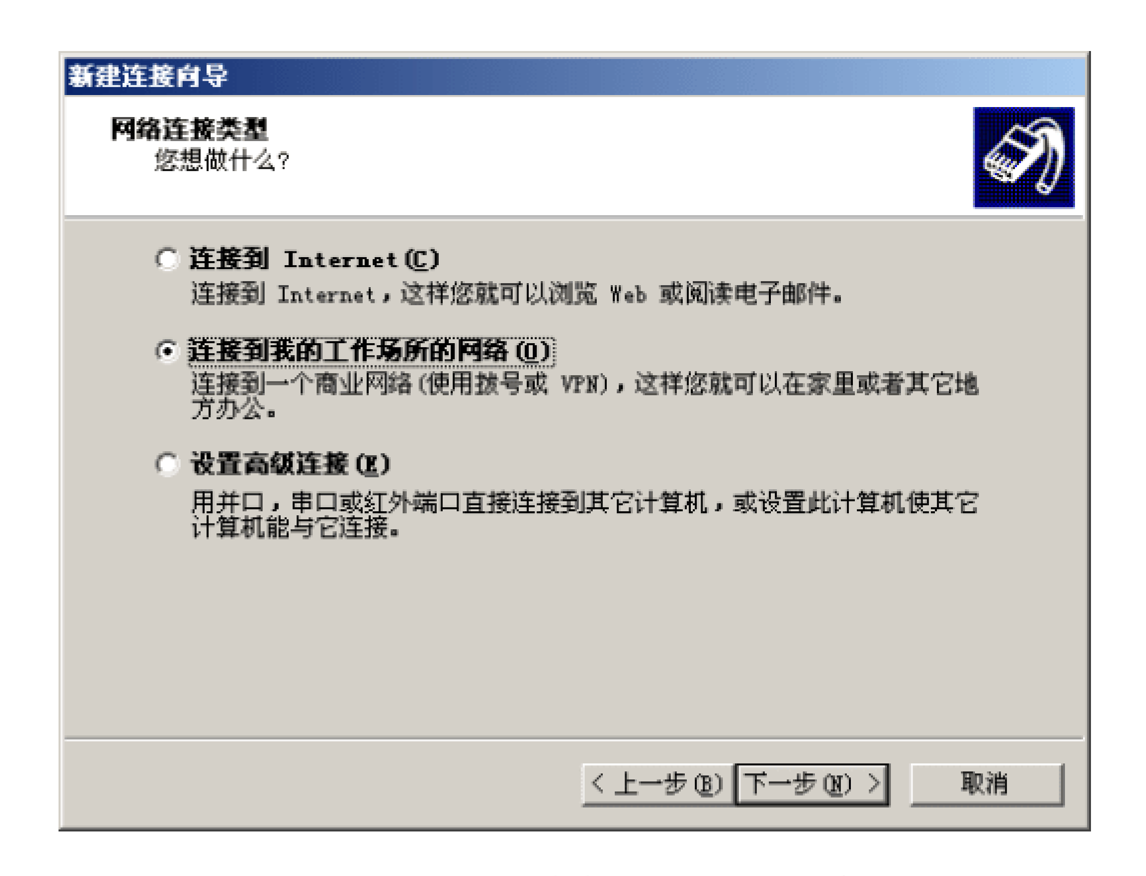


图 7-24 网络连接类型设置窗口

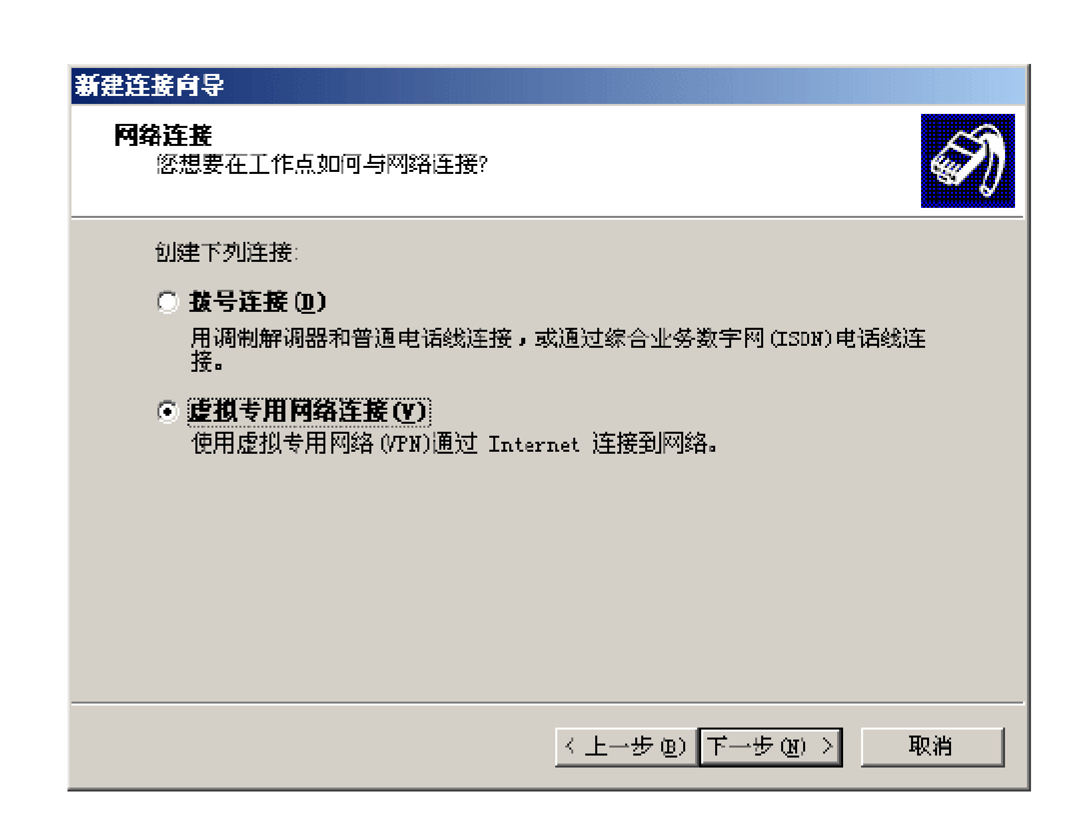


图 7-25 连接方式选择对话框

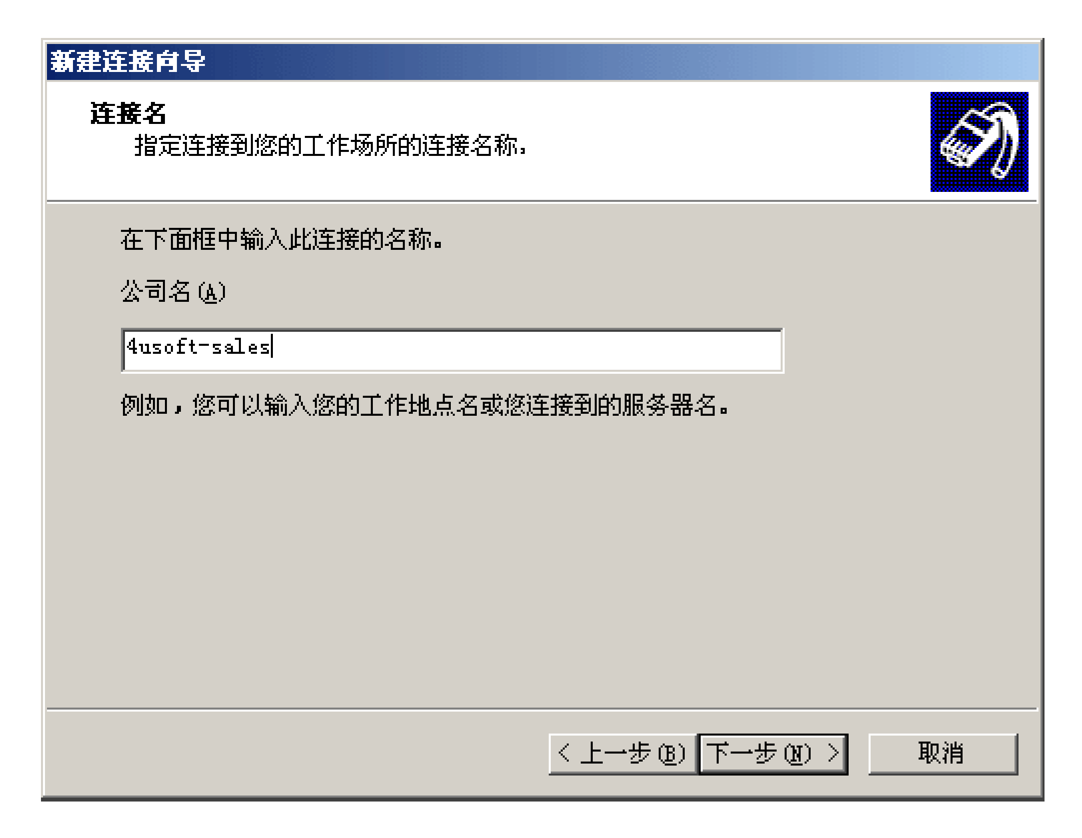


图 7-26 连接名设置对话框

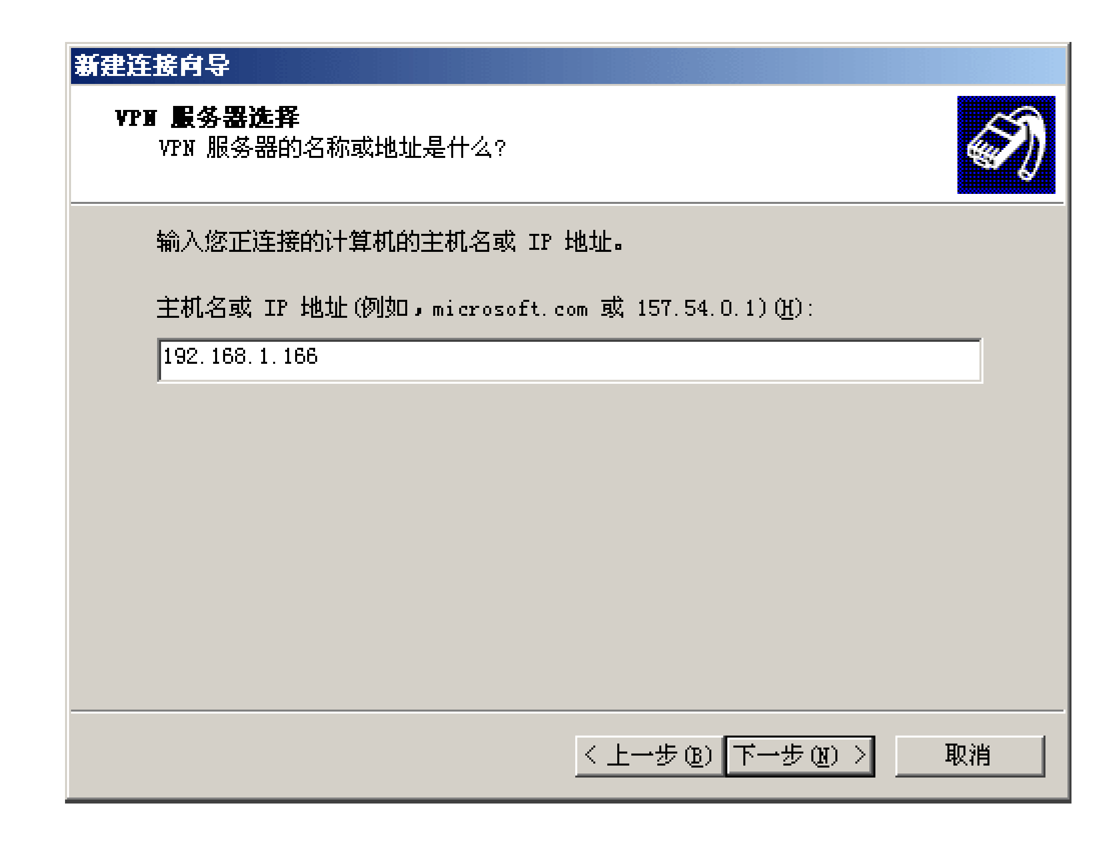


图 7-27 VPN 服务器设置

（6）设置好 VPN 服务器的主机名或者 IP 地址后，单击“下一步”按钮，出现可用连接用户设置对话框，如图 7-28 所示。

（7）选择“只是我使用”单选框，单击“下一步”按钮，出现完成设置对话框，如图 7-29 所示。

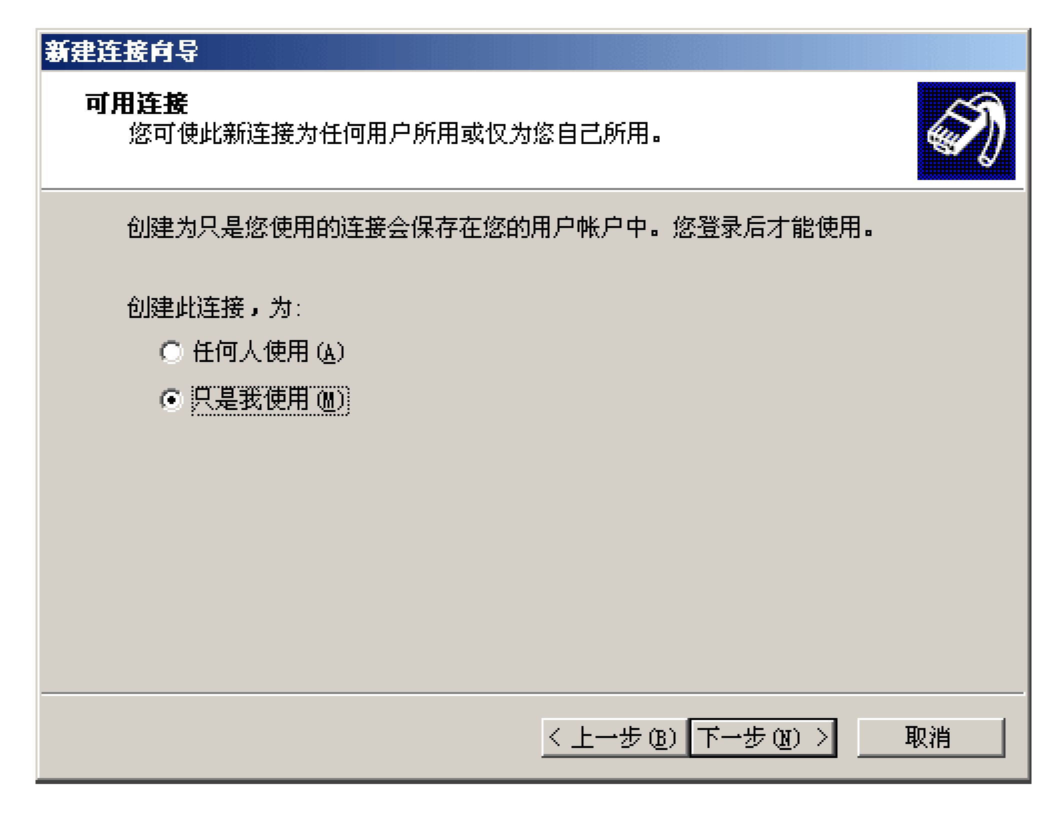


图 7-28 选择可用连接用户



图 7-29 设置完成对话框

（8）选择“在我的桌面上添加一个到此连接的快捷方式”复选框，单击“完成”按钮，完成对 VPN 服务器连接的设置，出现连接 VPN 服务器的窗口，如图 7-30 所示。

（9）在连接 VPN 服务器对话框上，输入用于拨入 VPN 的用户名和密码，然后单击“连

接”按钮。系统会建立一个到 VPN 服务器的连接，VPN 连接成功后，你可以单击任务栏弹出的“气球”以获得 VPN 连接的详细信息，如图 7-31 所示。



图 7-30　连接 VPN 服务器窗口

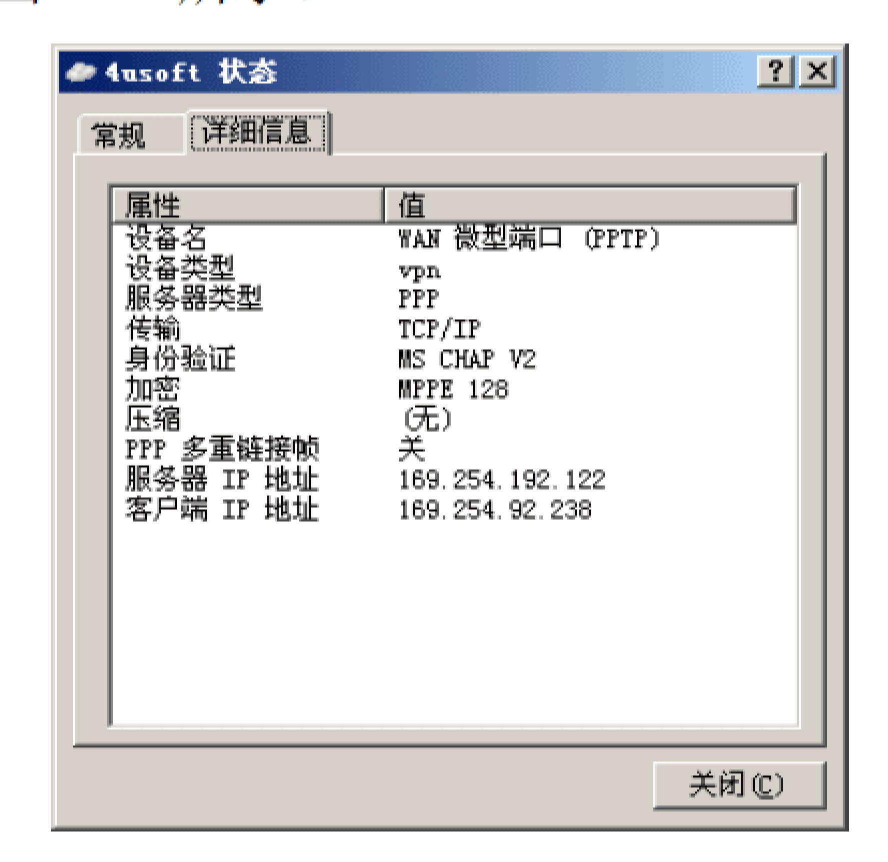


图 7-31　VPN 连接属性窗口

（10）打开浏览器，访问内部网络中的 VPN 服务器上的 Web 服务，出现访问成功的窗口显示，如图 7-32 所示。

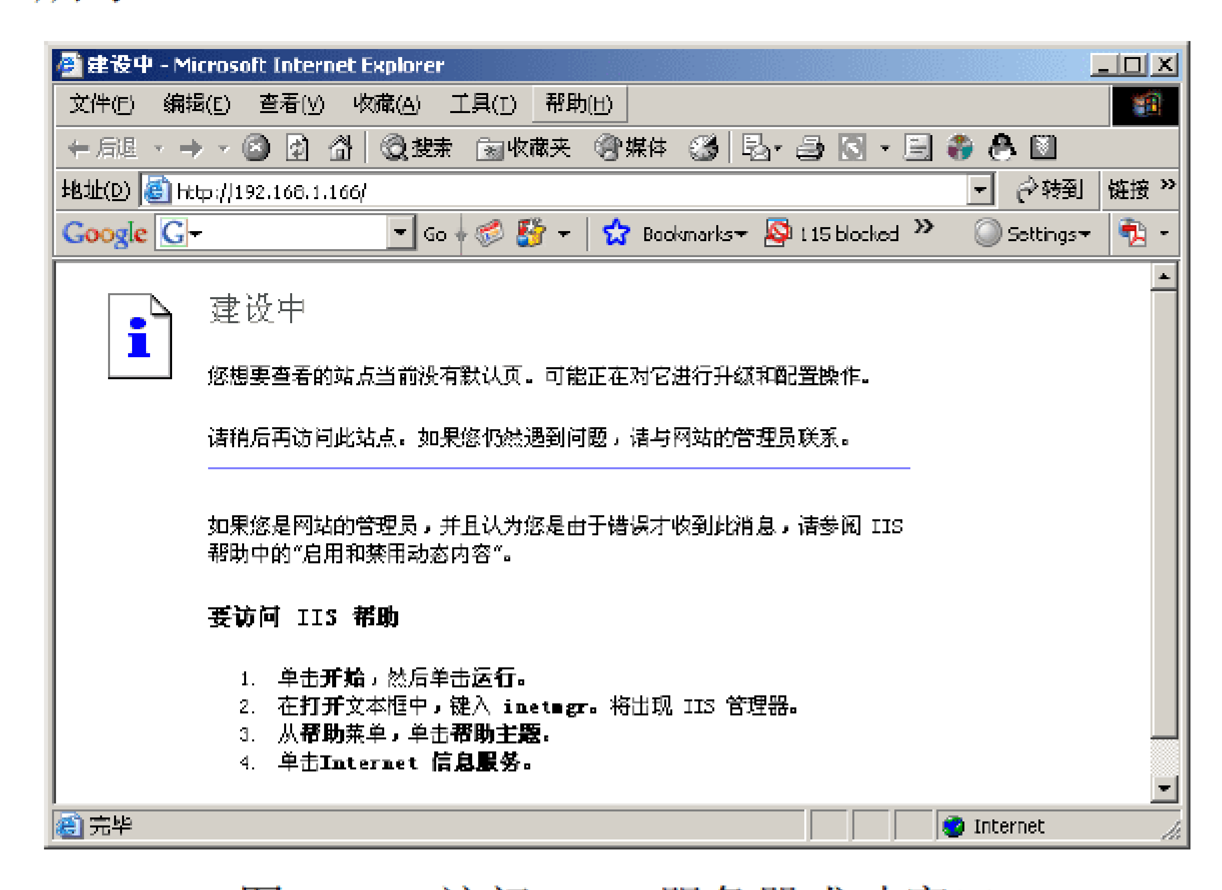


图 7-32　访问 VPN 服务器成功窗口

7.4　安全审计

网络给我们带来了非常广泛的方便，使得我们能够在网络存在的地方非常方便地发送和接收信息，同时，也给我们带来了安全风险，通过对日常的计算机操作行为进行安全审计，可以有效防止某些特定人为造成的信息泄密问题。

1．邮件安全审计

（1）监视并记录通过 OutLook Foxmail 等工具接收/发送邮件的邮件正文和附件；

（2）监视并记录通过 Web 页面发送的 Web 邮件内容和附件；

（3）控制外发邮件的大小；

（4）对邮箱的过滤，限定只能对某些邮箱进行发送；

（5）限制收发邮件的端口；

（6）使用延迟发送技术，等待邮件被审核后，再决定是否允许发送。

2．聊天工具审计

（1）监视 MSN Messenger /Yahoo Messenger /ICQ 等聊天工具的聊天内容；监视发送和接收到的消息以及文件；

（2）有效控制聊天软件的使用权。

3．上网安全审计

（1）记录浏览过的网站 URL；

（2）记录通过 Web 方式对外发送的信息；

（3）对网站建立黑白名单并建立多种过滤库，禁止浏览无关信息；

（4）限制某些计算机的上网时间；

（5）可控制下载某些类型的文件。

4．其他协议的审计

（1）FTP 详细命令监控/FTP 上传文件内容记录；

（2）Telnet 详细命令记录；

（3）Netbios 命令监控。

5．上网流量审计

（1）可实时看到每台上网机器的网络流量；

（2）可统计每台机器在某段时间的上网流量；

（3）可限制每台机器的上网流量。

7.5 企业广域网安全

对于大型企业来说，面对分布于不同地点或不同城市的分支机构，其安全不再仅仅局限于局域网，如何确保广域网的安全也成为一个迫切需要考虑的难题。

对于大型企业来说，它的分支机构可能分布于一座城市的不同地点，甚至于分布在不同的城市。那么对于这样的一个大型企业，它的网络安全问题就不仅局限于局域网的安全，还涉及到广域网的安全问题。下面向大家阐述一下大型企业的广域网络的安全策略。

1．确保骨干网数据畅通

省级分支机构连接到总部和地市级分支机构的网络是整个系统的骨干网络。该网络必须保证数据畅通，能够快速转发数据。为此，骨干网络可以采用两个独立的电信运营商的线路，连接到省级分支机构的两台主干路由器上，其中一条为电信的线路，另外一条为联通或广电网络的线路。省级分支机构到下属各地市级分支机构的数据通信采用 QoS 自动控制数据流量，实现负载均衡。在正常情况下，生产的数据在电信的线路上传输，而办公的数据则在联通或广电网络的线路上传输。一旦某一条线路出现中断，其上传输的数据会自动转移到另一条线路上，实现两条线路自动热备份。

2．使用 DDN/ISDN 冗余备份

省级分支机构到下属各营业网点的线路采用了 3 条电信的 155M ATM 线路，将此 155M 线路划分为 2M 的时隙分别连接到各下属的 100 多个营业网点。各营业网点租用了电信的 2M SDH 线路与省级相连，同时我们还在各营业网点租用了 DDN 或 ISDN 的线路作为对 2M

线路的备份。一旦 2M 线路出现故障，DDN 线路或 ISDN 线路将自动启用，保证各营业网点业务的正常运行。

3．核心网络设备做好应急方案

省级分支机构采用两台 Cisco 7206 路由器与总部连接，采用两台 Cisco 7507 与下属地市级分支机构连接。这些核心网络设备一旦出现故障将严重影响业务的安全生产，因此必须防患于未然，针对每一台核心网络设备制订出相应的应急处理方案，将故障的影响排除到最小，这是网络安全策略的重中之重。

4．传输数据采用加密技术

加密型网络安全技术的基本思想是不依赖于网络中数据通道的安全性来实现网络系统的安全，而是通过对网络数据的加密来保障网络的安全可靠性。数据加密技术可以分为三类：对称型加密、非对称型加密和不可逆加密。其中不可逆加密算法不存在密钥保管和分发问题，适用于分布式网络系统，但是其加密计算量相当可观。近年来，随着计算机系统性能的不断提高，不可逆加密算法的应用逐渐增加，常用的如 RSA 公司的 MD5 和美国国家标准局的 SHS。省级分支机构的路由器上采用了路由协议 MD5 认证。

5．应用防病毒访问控制列表

在省级分支机构路由器广域网端口上应用防病毒访问控制列表，可以避免个别区域网感染的一些病毒通过广域网传播到另一局域网。

如在广域网端口上应用包含以下内容的访问控制列表：

（1）ip access-list extended virus；

（2）deny tcp any any eq 137；

（3）deny tcp any any eq 138；

（4）deny tcp any any eq 139；

（5）deny tcp any any eq 1433；

（6）deny tcp any any eq 1434。

6．使用外联专用路由器

随着各项中间业务的拓展，与合作伙伴的网络连接越来越多，各种应用交错于网络中。因此，采取安全保护措施，确保自身网络的安全必须予以高度重视。

网络和外联单位的外网互联边界，必须和内部网络的核心路由器隔离，外网边界集中到一台专用的外网路由器上，便于网络安全的管理及安全防护策略的实施。

针对外联网络专用服务器，可以采取以下安全策略：

（1）在外网路由器上仅采用静态路由，保证路由安全性；

（2）外网路由器必须关闭 CDP，以免泄露外网路由器信息；

（3）启用路由器 ACS 用户认证；

（4）基于多重保护原则，外网路由器也启用 ACL，和防火墙安全策略保持一致，确保在防火墙发生故障时还保持相当的防护。

省级分支机构采取 Cisco PIX 550 防火墙在物理上隔离内网和外网，使内网和外网的访问都要通过防火墙的检查，以达到控制内网和外网数据流的目的，从而增强外网安全性，保证了外网边界能够防范和抵御大部分常见的黑客攻击手段。

在部署防火墙时，也应考虑一些具体的安全策略，具体如下。

（1）外网访问内网的安全策略

对外网采用静态路由，精确到主机位，且不使用默认路由；外网指定主机通过 MIP 地址来访问内网中间业务服务器；外网指定主机只允许访问内网中间业务服务器的应用端口。

（2）内网访问外网的安全策略

对内采用静态路由，精确到主机位，且不使用默认路由；内网中间业务服务器访问外网时将转换成相应的 MIP，从而屏蔽内网地址；内网中间业务服务器将只访问外网指定主机的应用端口。

（3）防火墙自身安全策略

设定防火墙的一个端口为内网端口。使用专用的管理 VLAN 地址段。仅指定该端口为管理端口，其他端口均不允许提供任何管理防火墙的服务。仅指定专用管理 VLAN 内的个别或部分 IP 地址允许对防火墙进行管理。

7．加强对外联拨号的监控

防火墙的设置解决了网络出口的安全问题，但是一旦局域网内的用户通过非法拨号到外网，外网的黑客便可以轻易地攻破这台拨号的计算机，从而进一步攻入内网。局域网内经常有用户通过拨号非法外联，给入侵者提供了一个后门，因此必须使用防非法外联软件，对网络连接状况进行实时监控。

7.6 电子商务安全

电子商务的安全不仅仅是狭义上的网络安全，比如防病毒、防黑客、入侵检测等，从广义上讲还包括信息的完整性以及交易双方身份的不可抵赖性，从这种意义上来说，电子商务的安全涵盖面比一般的网络安全要广泛得多，从整体上可分为两大部分：计算机网络安全和商务交易安全。

7.6.1 电子商务安全策略

实现电子商务的关键是要保证商务活动过程中系统的安全性，即保证基于互联网的电子交易过程与传统交易的方式一样安全可靠。电子商务的安全主要采用数据加密和身份认证技术。

1．认证系统

电子商务的关键是安全，网上安全交易的基础是数字证书。要建立安全的电子商务系统，必须首先建立一个稳固、健全的 CA；否则，一切网上的交易都没有安全保障。

2．认证系统的基本原理

传统的对称密钥算法具有加密强度高、运算速度快的优点，但密钥的传递与管理问题限制了它的一些应用。为解决此问题，七十年代密码界出现了公开密钥算法，该算法使用一对密钥即一个私钥和一个公钥，其对应关系是唯一的，公钥对外公开，私钥个人秘密保存。一般用公钥来进行加密，用私钥来进行签名；同时私钥用来解密，公钥用来验证签名。算法的加密强度主要取决于选定的密钥长度。

RSA 算法是公开密钥算法中研究最为深入，使用最为广泛的算法，为大多数国家地区的官方或非官方所采用。利用 RSA 公开密钥算法在密钥自动管理、数字签名、身份识别等

方面的特性，可建立一个为用户的公开密钥提供担保的可信的第三方认证系统。这个可信的第三方认证系统也称为 CA，CA 为用户发放电子证书，用户之间（比如网银服务器和某客户之间）利用证书来保证信息安全性和双方身份的合法性。

3．系统结构

所谓系统就是一个大的网络环境。系统从功能上基本可以划分为 CA、RA 和 WP。

核心系统和 CA 放在一个单独的封闭空间中，为了保证运行的绝对安全，其人员及制度都应有严格的规定，并且系统设计为离线网络。CA 的功能是在收到来自 RA 的证书请求时颁发证书。一般的个人证书发放过程都是自动进行，无须人工干预。

以网上银行为例，证书的登记机构 Register Authority，简称 RA，分散在各个网上银行的地区中心。RA 与网上银行中心有机结合，接受客户申请，并审批申请，把证书正式请求通过银行企业内部网发送给 CA 中心。RA 与 CA 双方的通信报文也通过 RSA 进行加密，确保安全。系统的分布式结构适于新业务网点的开设，具有较好的扩充性。通信协议为 TCP/IP。

证书的公布系统 Web Publisher，简称 WP，置于 Internet 网上，是普通用户和 CA 直接交流的界面。对用户来讲它相当于一个在线的证书数据库。用户的证书颁发之后，CA 用 E-mail 通知用户，然后用户须用浏览器从这里下载证书。

4．SSL 协议

SSL 协议是 Netscape 公司在网络传输层之上提供的一种基于 RSA 和保密密钥的用于浏览器和 Web 服务器之间的安全连接技术。它被视为 Internet 上 Web 浏览器和服务器的标准安全性措施。SSL 提供了用于启动 TCP/IP 连接的安全性“信号交换”。这种信号交换导致客户和服务器同意将使用的安全性级别，并履行连接的任何身份验证要求。它通过数字签名和数字证书可实现浏览器和 Web 服务器双方的身份验证。在用数字证书对双方的身份验证后，双方就可以用保密密钥进行安全的会话了。

SSL 协议在应用层收发数据前，协商加密算法、连接密钥并认证通信双方，从而为应用层提供了安全的传输通道；在该通道上可透明加载任何高层应用协议（如 HTTP、FTP、TELNET 等）以保证应用层数据传输的安全性。SSL 协议独立于应用层协议，因此，在电子交易中被用来安全传送信用卡号码。

中国目前多家银行均采用 SSL 协议，如在目前中国的电子商务系统中能完成实时支付，用的最多的招行一网通采用的就是 SSL 协议。所以，从目前实际使用的情况看，SSL 还是人们最信赖的协议。

SSL 当初并不是为支持电子商务而设计的，所以在电子商务系统的应用中还存在很多弊端。它是一个面向连接的协议，在涉及多方的电子交易中，只能提供交易中客户与服务器间的双方认证，而电子商务往往是用户、网站、银行三家协作完成，SSL 协议并不能协调各方间的安全传输和信任关系；还有，购货时用户要输入通信地址，这样将可能使得用户收到大量垃圾信件。

因此，为了实现更加完善的电子交易，MasterCard 和 Visa 以及其他一些业界厂商制订并发布了 SET 协议。

5．SET 协议

SET 协议是针对开放网络上安全、有效的银行卡交易，由 Visa 和 Mastercard 联合研制

的，为 Internet 上卡支付交易提供高层的安全和反欺诈保证。

SET 协议保证了电子交易的机密性、数据完整性、身份的合法性和抗否认性。

SET 是专门为电子商务而设计的协议，虽然它在很多方面优于 SSL 协议，但仍然不能解决电子商务所遇到的全部问题。而且，SET 遭到有些银行的抵制，其前途如何，尚未得知。

7.6.2 电子商务安全技术

1. PKI 在电子商务中的作用

公钥基础设施 PKI（Public-key Infrastructure）是解决信任和加密问题的基本解决方案。

网络环境下，特别是 Internet 环境下的电子交易往往是在互不相识的消费者和销售商或企业和企业之间发生的。对“互不相识”更加准确的描述应当是“互不信任”。公钥加密技术的发明使得互不相识的两个人（或主体）可以安全地通信。在规模不大的网络或较为封闭的网络中，通信主体可以通过 KDC 这一类的密钥分发或管理中心可靠地获得通信对方的公钥，即通过 KDC 和协议可以实现安全的公钥分发。但是在较大规模的网络环境中，特别是在 Internet 环境下，KDC 不再适用，因而这种环境下的公钥分发问题成为最突出的问题。可靠地获得通信对方的公钥的问题在网络环境下就是信任的问题，因而大规模网络中最突出的问题也就是信任的问题。PKI 的本质就是实现了大规模网络中的公钥分发问题，建立了大规模网络中的信任基础。

PKI 是创建、管理、存储、分发和取消基于公钥加密的公钥证书所需要的一套硬件、软件、人、策略和过程的集合。PKI 框架中的核心元素是公钥证书；PKI 的核心实施者是认证中心（CA，Certification Authority）。公钥证书是 CA 对主体的公钥和主体的其他属性做签名而形成的一种信息结构。公钥证书将主体的公钥以及其他属性与主体的身份绑定。主体之间对彼此的信任，也即对彼此公钥和其他属性的相信，建立在主体对 CA 的信任的基础上。尽管两个主体互不认识，但只要二者都通过同一个 CA 的考察并获得该 CA 签发的证书，则二者通过成功地验证彼此的证书的正确性、有效性，就可以建立信任关系。当然，在实际网络环境中不可能只有一个 CA，因此 PKI 给出了两种传统的信任模型：层次信任模型和网状信任模型，以解决不同的管理域（即一个 CA 所管理的域）中的主体间的信任问题。此外，美国和加拿大还推出了桥 CA 信任模型。桥 CA 的目的是连接多个 PKI，建立 PKI 间的信任关系和实现 PKI 间的互操作。这些 PKI 的信任模型可以是任何传统类型的信任模型。桥 CA 与各个 PKI 中被选做主 CA（principal CA）的 CA 做交叉认证。若一个 PKI 用层次信任模型实现，则桥 CA 与其根 CA 建立交叉认证；若一个 PKI 用网状信任模型实现，则桥 CA 只与其中的一个 CA 建立交叉认证。桥 CA 只是一个中介，它不直接向用户发证书，也不作为一个根信任点。

PKI 很好地解决了大规模网络环境中的信任这一难题，从而保证了验证、机密性、完整性和非否认的有效实施。验证、机密性、完整性和非否认都是电子商务所必需的安全服务。

虽然 PKI 建立了大规模网络环境中的信任和安全的公钥分发的理论基础，但实际中 PKI 的成功实施将更多地取决于管理、法律、商业等方面的合理约定，对于电子商务也不例外。

2．数字签名与 PKI

目前得到认可并被广泛应用的数字签名方案都是基于公钥密码学的。简单地讲，数字签名就是签名者利用自己的私钥对数据的摘要进行的运算，任何人可以用签名者的公钥对数字签名进行验证。在数字化世界中，数字签名作为手写签名的替代形式，具有不可替代的地位：消息是可信的，消息是经签名者认可的；消息是完整的，经过签名的消息不能发生任何改动；签名不可重用，签名结果是关于消息的函数，不能用于其他消息；签名不可否认，签名结果不能为他人伪造，因而签名者不能否认其签名。

在实际中，若要应用数字签名技术，必须保证两点：即私钥的保密性和公钥的公开性。私钥的保密性由用户自己来完成，目前认为通过智能卡来保存是最安全的方式。而公钥的公开性，即任何人都能够知道其他所有人的可信公钥，是应用数字签名的最大困难。通过可信第三方——认证机构（CA）颁发数字证书，是解决公钥分发问题的最有效途径。关于数字证书的生成、颁发、管理、撤销过程中所涉及的所有软件、硬件、过程规范、法律法规、人员等统称为公钥基础设施（PKI）。PKI 提供了一种机制，使得验证者能够确信签名者公钥的真实性，因此，PKI 是实现数字签名的基础。

3．虚拟专用网（VPN）

这是用于 Internet 交易的一种专用网络，它可以在两个系统之间建立安全的信道（或隧道），用于电子数据交换（EDI）。它与信用卡交易和客户发送订单交易不同，因为在 VPN 中，双方的数据通信量要大得多，而且通信的双方彼此都很熟悉。这意味着可以使用复杂的专用加密和认证技术，只要通信的双方默认即可，没有必要为所有的 VPN 进行统一的加密和认证。

尽管 VPN 是进行电子商务的一种十分理想的形式，而且它使用的加密和认证技术可以大大提高电子商务的安全性，但它的安全问题仍不容忽视。黑客们都以能够攻破那些“安全”的网络为乐，因此，越是安全的网络就越容易受到黑客的攻击。对此，现有的或正在开发的数据隧道系统可以进一步增加 VPN 的安全性，因而能够保证数据的保密性和可用性。

4．对加密算法的控制

保证电子商务安全的最重要的一点就是使用加密技术对敏感的信息进行加密。现在，一些专用密钥加密（如 TripleDES、IDEA、RC4 和 RC5）和公钥加密（如 RSA、SEEK、PGP 和 EU）可用来保证电子商务的保密性、完整性、真实性和非否认服务。然而，这些技术的广泛使用却不是一件容易的事情。

密码学界有一句名言：加密技术本身都很优秀，但是它们实现起来却往往很不理想。现在虽然有多种加密标准，但人们真正需要的是针对企业环境开发的标准加密系统。加密技术的多样化为人们提供了更多的选择余地，但也同时带来了一个兼容性问题，不同的商家可能会采用不同的标准。针对这个问题，Netscape 推出了 SSL（安全套接层），主要目的是提供 Internet 上的安全通信服务，其版本已升级到 SSL3.0。虽然它能够对信用卡和个人信息提供较强的保护，但加密技术向来是由国家控制的，SSL 的出口自然受到美国国家安全局（NSA）的限制。目前，美国的商家一般都可以使用 128 位的 SSL，但美国只允许加密密钥为 40 位以下的算法出口。虽然 40 位的 SSL 也具有一定的加密强度，但它的安全系数显然比 128 位的 SSL 要低得多。据报载，最近美国加州已经有人成功地破译了 40 位

的 SSL，这已引起了人们的广泛关注。美国以外的国家很难真正在电子商务中充分利用 SSL，这不能不说是一种遗憾。

当前，在信用卡交易方面，商家可以通过 SSL 在 Web 上实现对信用卡订单的加密，Navigator 和 Internet Explorer 浏览器都支持 SSL。虽然它是基于强公钥加密技术以及 RSA 的专用密钥序列密码，可以为电子商务提供较强的加密保护，但 SSL 在全球的大规模使用还有一定的难度。

7.6.3 电子商务安全规范

电子商务安全规范可分为安全、认证两方面的规范。

1. 安全规范

当前电子商务的安全规范包括加密算法、报文摘要算法、安全通信协议等方面的规范。

（1）加密算法

基本加密算法有两种，即对称密钥加密和非对称密钥加密，用于保证电子商务中数据的保密性、完整性、真实性和非抵赖服务。

（2）报文摘要算法

报文摘要算法即采用单向哈希算法将需要加密的明文进行摘要，而产生的具有固定长度的单向散列（哈希）值。其中，散列函数是将一个不同长度的报文转换成一个数字串（即报文摘要）的公式，该函数不需要密钥，公式决定了报文摘要的长度。报文摘要和非对称加密一起，提供数字签名的方法。报文摘要算法主要有安全散列标准、MD2 系列标准。

（3）加密通信协议（SSL）

安全套接层协议是一种保护 Web 通信的工业标准，主要目的是提供 INTERNET 上的安全通信服务，是基于强公钥加密技术以及 RSA 的专用密钥序列密码，能够对信用卡和个人信息、电子商务提供较强的加密保护。SSL 在建立连接过程上采用公开密钥，在会话过程中使用专有密钥。SSL 的缺陷是只能保证传输过程的安全，无法知道在传输过程中是否受到窃听，黑客可以此破译 SSL 的加密数据，破坏和盗窃 Web 信息。新的 SSL 协议被命名为 TLS（Transport Layer Security），安全可靠性可有所提高，但仍不能消除原有技术上的基本缺陷。

2. 认证规范

（1）数字签名

数字签名是公开密钥加密技术的一种应用，是指用发送方的私有密钥加密报文摘要，然后将其与原始的信息附加在一起，合称为数字签名。其使用方式是：报文的发送方从报文文本中生成一个 128 位或 160 位的单向散列值（或报文摘要），并用自己的私有密钥对这个散列值进行加密，形成发送方的数字签名；然后，将这个数字签名作为报文的附件和报文一起发送给报文的接收方；报文的接收方首先从接收到的原始报文中计算出 128 位的散列值（或报文摘要），接着再用发送方的公开密钥来对报文附加的数字签名进行解密；如果这两个散列值相同，那么接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别与验证，保证报文的完整性、权威性和发送者对所发报文的不可抵赖性。数字签名机制提供了一种鉴别方法，普遍用于银行、电子贸易等，以解决伪造、抵

赖、冒充、篡改等问题。

（2）数字证书

“数字证书”是一个经证书认证中心（CA）数字签名的、包含证书申请者（公开密钥拥有者）个人信息及其公开密钥的文件。基于公开密钥体制（PKI）的数字证书是电子商务安全体系的核心，用途是利用公共密钥加密系统来保护与验证公众的密钥。CA 对申请者所提供的信息进行验证，然后通过向电子商务各参与方签发数字证书，来确认各方的身份，保证网上支付的安全性。

证书的格式遵循 X.509 标准。X.509 证书包括有关证书拥有的个人或实体的信息及证书颁发机构的可选信息。实体信息包括实体名称、公用密钥、公用密钥运算法和可选的唯一主体 id。目前，X.509 标准已在编排公共密钥格式方面被广泛接受，已用于许多网络安全应用程序，其中包括 IP 安全（Ipsec）、安全套接层（SSL）、安全电子交易（SET）、安全多媒体 INTERNET 邮件扩展（S/MIME）等。

（3）密钥管理机制（PKI）

公钥基础结构(Public Key Infrastructure，简称 PKI)采用证书管理公钥，即结合 X.509 标准中的鉴别框架（AuthenticationFramework）来实现密钥管理，通过 CA 把用户的公钥及其他标识信息捆绑在一起，在 INTERNET 上验证用户的身份，保证网上数据的保密性和完整性。

PKIX（PublicKeyInfrastructureonX.509，简称 PKIX）系列标准由 IETFPKIX 工作小组制定，定义了 X.509 证书在 INTERNET 上的使用，证书的生成、发布和获取，各种产生和分发密钥的机制，以及怎样实现这些标准的轮廓结构等。

7.6.4　Windows 2000 的安全机制

1．Windows 2000 中的验证协议

Windows 2000 中有两种验证协议，即 Kerberos 和公用密钥体制（Public Key Infrastructure，PKI）。Kerberos 是对称密钥，而 PKI 是非对称密钥。用的较多的是公用密钥体制。

公用密钥基本体系是一个数字认证、证书授权和其他注册授权系统。使用公用密钥密码检验及检证电子商务中所涉及的每个机构的有效性。公用密钥基本体系的标准仍处于发展阶段，尽管它们作为电子商务的一个必要组成部分已得到广泛使用。

Windows 2000 公钥基础结构的证书基本上是一个由权威发布的电子声明，其作用在于担保证书持有者的身份。证书将公用密码与持有相应私有密钥的个人、机器或服务的身份绑定在一起。证书由各种公用密钥安全服务和应用程序提供，为非安全网（如 internet）提供数据验证、数据完整性和安全通信。

2．Windows 2000 Server 的证书服务器

Windows 2000 Server 中有一个部件是证书服务器（Certificate Server），通过认证服务器，企业可以为用户颁发各种电子证书，比如用于网上购物的安全通道协议(SSL)使用的证书，用于加密本地文件的证书等等。认证服务器还管理证书的失效，发布失效证书列表等。每个用户或计算机都有自己的一个证书管理器，其中既放置着自己从 CA 申请获得的证书，也有自己所信任的 CA 的根证书。

Windows 2000 基于证书的过程所使用的标准证书格式是 X.509v3，保证了与其他系统的互操作性。目前常用的是 SSL（安全通道协议）的方式，即设置 IIS 就某些特定的文件或文件目录需要访问者提供客户端证书；除非拥有电子证书及相应的私钥，一个访问者的浏览器无法获得这些文件和文件目录。SSL 的方式体现在浏览器的访问栏上，应该是 https 而不是普通的 http。

Windows 2000 server 证书服务是 Windows 2000 中的组件，证书服务用于创建和管理证书颁发机构（CA）。证书颁发机构负责建立和担保证书持有者的身份。证书颁发机构还会在证书失效时，将其撤销并发布证书撤销列表，供证书检验机构使用。最简单的公用密钥基本体系只有一个证书颁发机构。事实上，大多数配置公用密钥基本体系的组织使用多个证书颁发机构，并将其有组织地形成证书分层结构。

Windows 2000 的证书服务按证书颁发机构类型分为：

（1）企业根 CA，是企业中最受信任的证书颁发机构，应该在网络上的其他证书颁发机构之前安装，需要 Active Directory。

（2）企业从属 CA，是标准证书颁发机构可以给企业中的任何用户或机器颁发证书，必须从企业中的另一个证书颁发机构获取证书颁发机构证书，需要 Active Directory。

（3）独立根 CA，是证书颁发机构体系中最受信任的证书颁发机构，不需要 Active Directory。

（4）独立从属 CA，是标准的证书颁发机构可以给任何用户或机器颁发证书；必须从另一个证书颁发机构获取证书颁发机构证书，不需要 Active Directory。

3. 智能卡支持

在 Windows 2000 中，微软为用户还提供了一套智能卡的结构。智能卡因其高安全性和轻便的可移动性，势必将发展成为类似鼠标/键盘一般计算机的标准外设。

当用户用 Internet Explorer 向一个认证中心申请电子证书时，就会有一对公钥和私钥自动产生出来；私钥可以存储在智能卡中，公钥和其他身份信息（比如姓名、电子邮件地址等）发给认证中心。如果认证中心批准该申请，那么包含公钥的电子证书就会被返回来，存储在智能卡中。

智能卡存储私钥和电子证书的做法，给最终用户提供了对自己安全信息的最大的控制，可以方便地从一台机器携带到另一台机器使用；可以在任何一个地点使用。一般来说，智能卡还会用一个个人密码(Pin)保护起来，在要求高安全性的场合，Pin 可以是一些生物信息，比如指纹等。

7.6.5 Windows 2000 下建立 CA 中心的具体操作过程

证书服务的一个单独组件是证书颁发机构的 Web 注册页。这些网页是在安装证书颁发机构时默认安装的，它允许证书请求者使用 Web 浏览器提出证书请求。此外，证书颁发机构网页可以安装在未安装证书颁发机构的 Windows 2000 服务器上，在这种情况下，网页用于向不希望直接访问证书颁发机构的用户服务。如果选择为组织创建定制网页访问 CA，则 Windows 2000 提供的网页可作为示例。现在我们以安装独立根证书为例，安装其他类型的相类似，只是选择其他证书的类型即可。要注意的是企业根 CA 和企业从属 CA 需要 ActiveDirectory。

1．安装独立的根证书颁发机构

（1）以管理员身份登录到系统。或者，如果您装有 ActiveDirectory，则以域管理员身份登录到系统。

（2）选择“开始”|“设置”|“控制面板”命令，在出现的“控制面板”窗口中，双击“添加/删除程序”，如图 7-33 所示。

（3）单击“添加/删除 Windows 组件”，出现“Windows 组件向导”对话框，如图 7-34 所示。



图 7-33　添加/删除组件窗口



图 7-34　“Windows 组件向导”对话框

（4）在“Windows 组件向导”对话框中，选中“证书服务”复选框。屏幕上将出现一个对话框，通知您计算机在安装证书服务之后不能更名且不能加入域或从域中删除，如图 7-35 所示。



图 7-35　提示对话框

（5）单击“是”按钮，然后单击“Windows 组件向导”对话框的“下一步”按钮，出现如图 7-36 所示。

（6）选择“独立根 CA”单选框，选择“高级选项”复选框，单击“下一步”按钮，出现如图 7-37 所示。

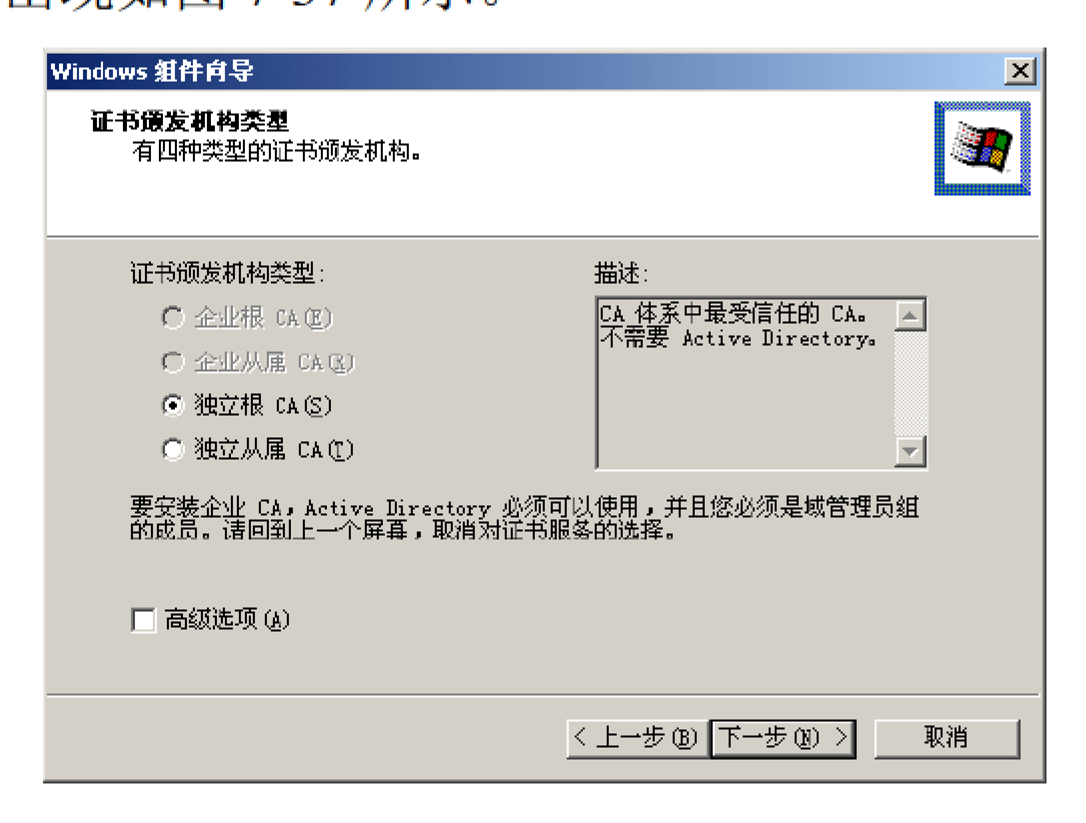


图 7-36　证书颁发机构类型选择

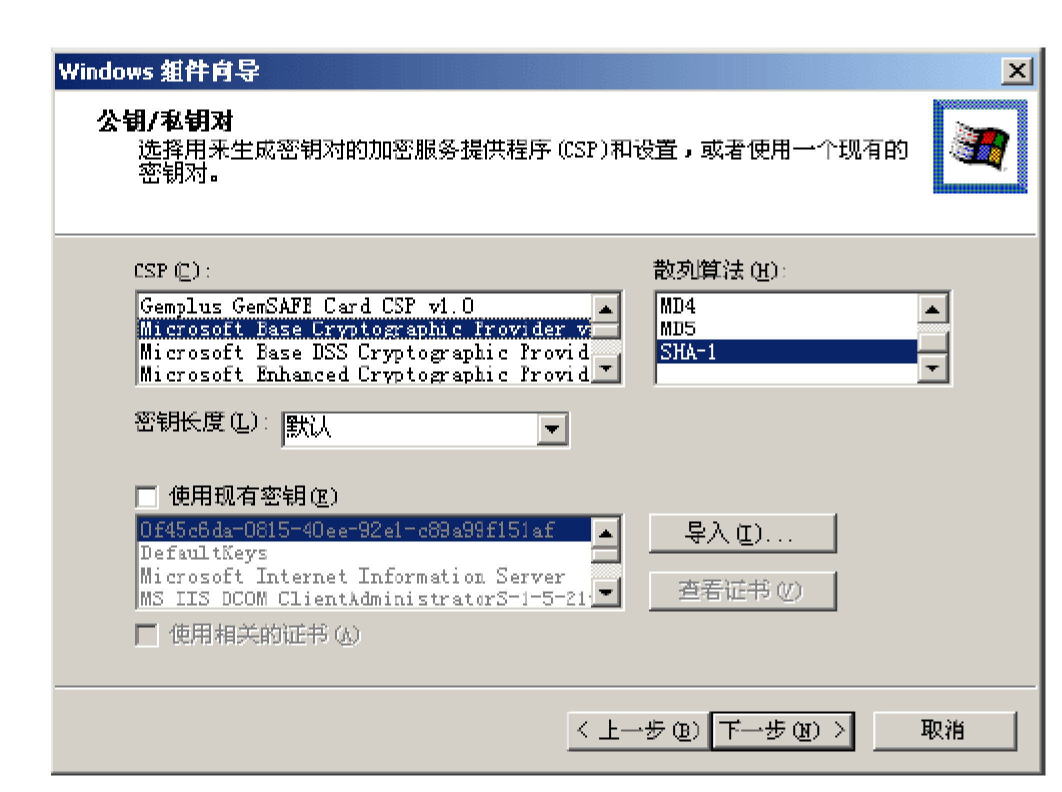


图 7-37　加密提供程序选择

（7）保持窗口默认设置，单击“下一步”按钮，出现 CA 标识信息设置窗口，如图 7-38 所示。

（8）设置 CA 标识信息，完成后单击“下一步”按钮，出现数据存储位置设置窗口，如图 7-39 所示。

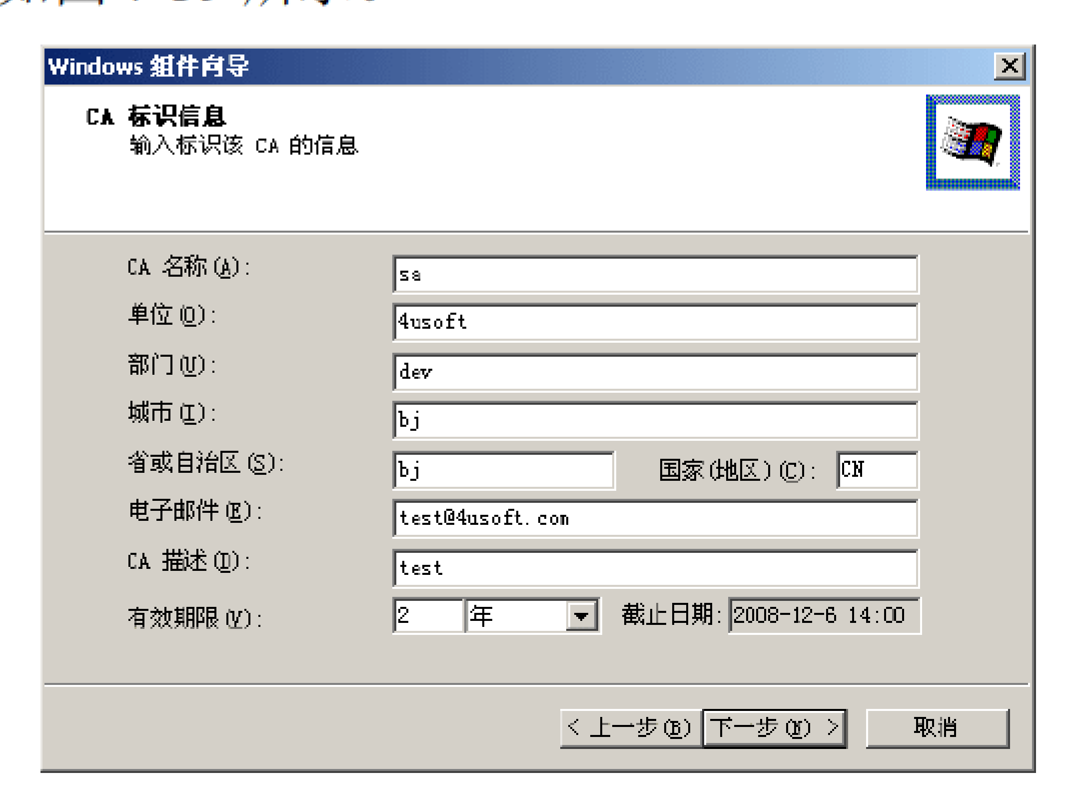


图 7-38　设置 CA 标识信息



图 7-39　数据存储位置设置窗口

（9）开始进行 CA 安装，通常需要操作系统的安装盘，完成后出现提示对话框，如图 7-40 所示。

2．设置安全性以访问证书颁发机构 Web 页

（1）以管理员身份登录到系统。

（2）选择“开始”|“程序”|“管理工具”|“Internet 服务管理器”命令，出现“IIS 信息服务”窗口，如图 7-41 所示。



图 7-40　完成安装提示对话框

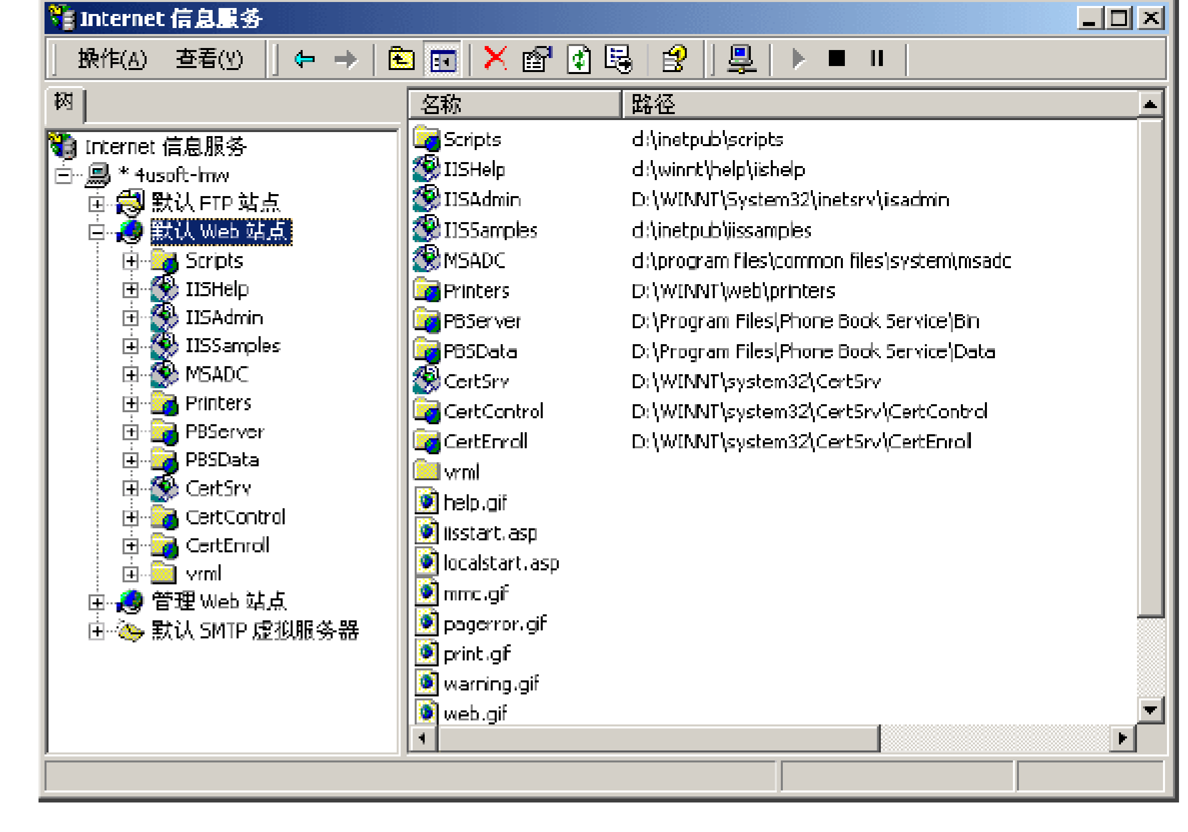


图 7-41　Internet 信息服务

（3）在“Internet 信息服务”窗口中，在窗口左边选择“默认 Web 站点”| CertSrv，右击 CertSrv 项，在弹出菜单中选择“属性”，如图 7-42 所示。

（4）选择“目录安全性”选项卡，在“匿名访问和验证控制”组合框中，单击“编辑”按钮，出现验证方法设置对话框，如图 7-43 所示。

（5）清除“集成 Windows 验证”之外的其他所有复选框，单击“确定”按钮，完成设置。

（6）在“Internet 信息服务”窗口左边，右击“默认 Web 站点”，在弹出菜单中选择“属性”命令，出现如图 7-44 所示。

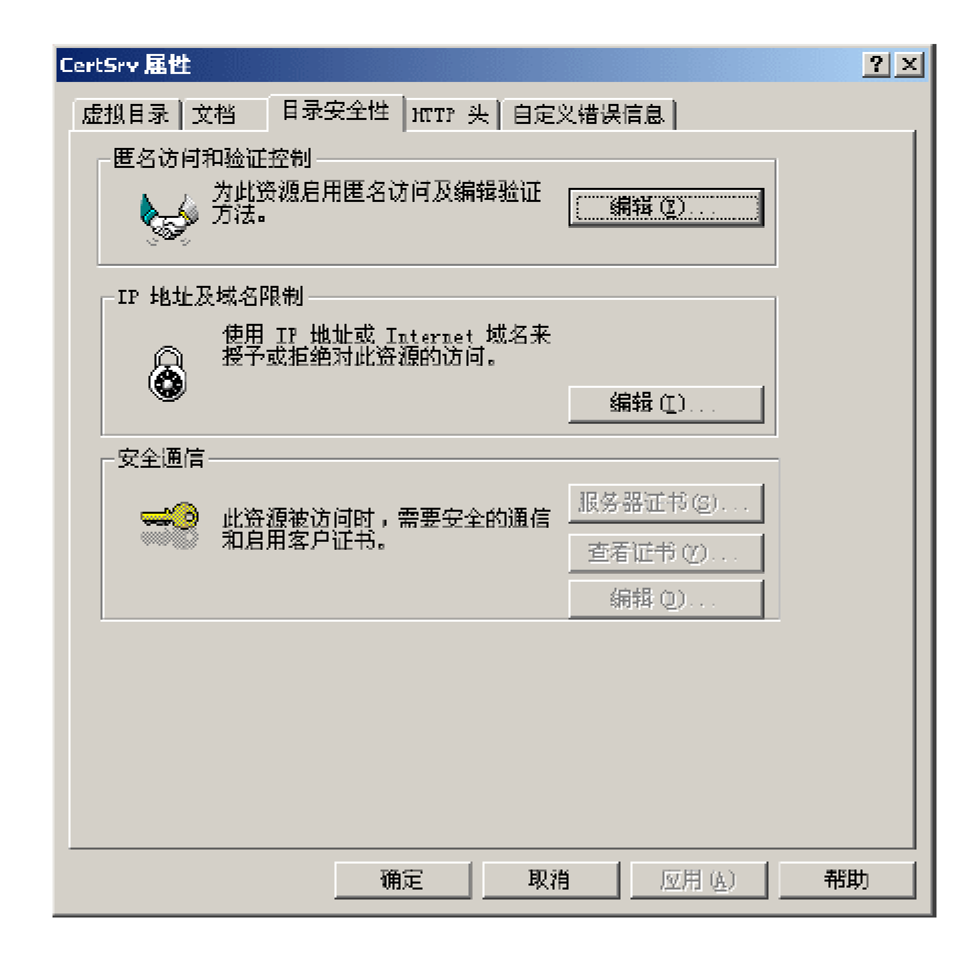



图 7-42　CertSrv 属性对话框

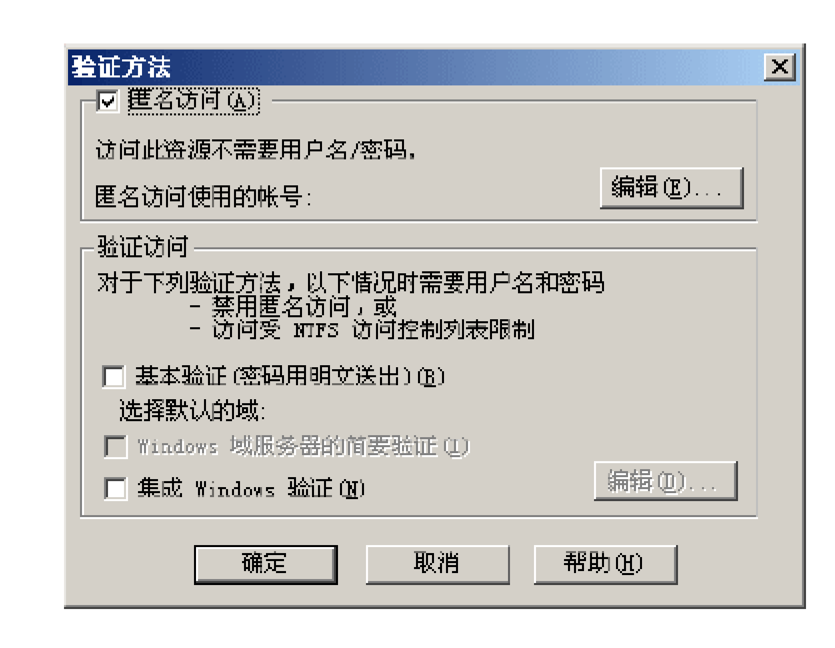


图 7-43　验证方法设置窗口

（7）在“IP 地址”文本框中输入计算机的 IP 地址，然后选择“文档”选项卡，将 Default.asp 设置为第一个文档，然后单击“确定”按钮。

（8）在 IE 地址栏中输入“http://设置的 IP/CertSrv”，出现 Microsoft 证书服务窗口，如图 7-45 所示。

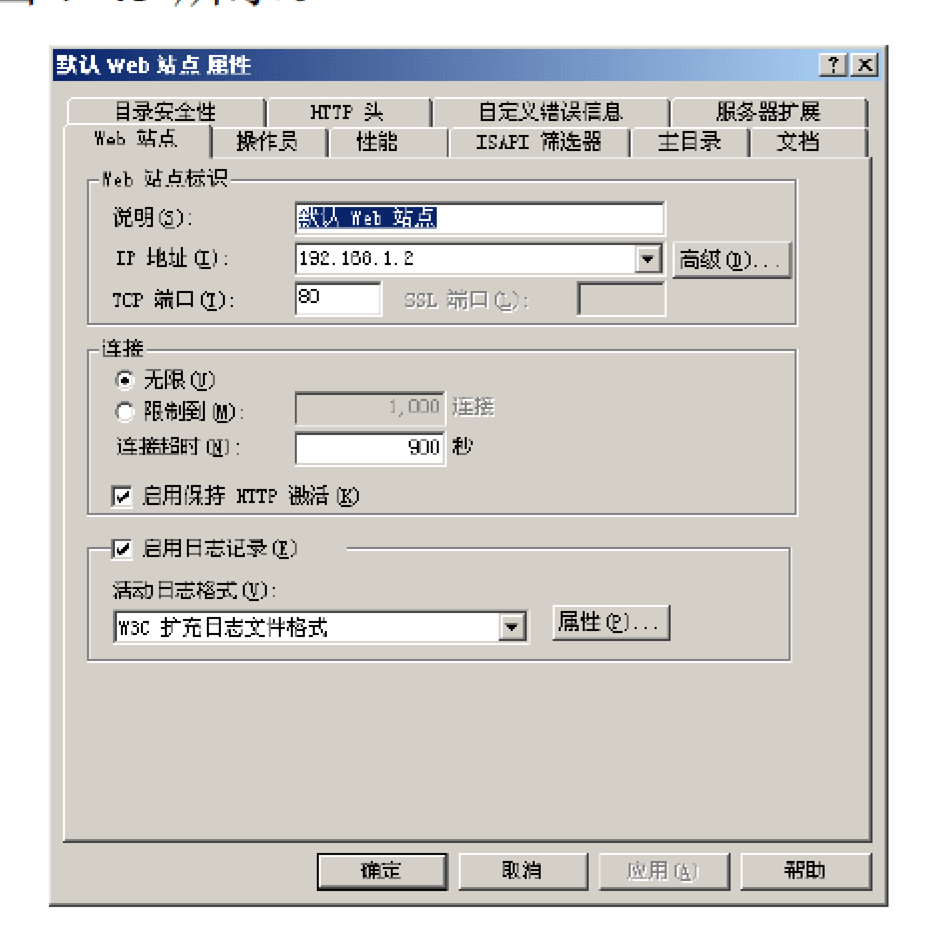


图 7-44　默认 Web 站点属性

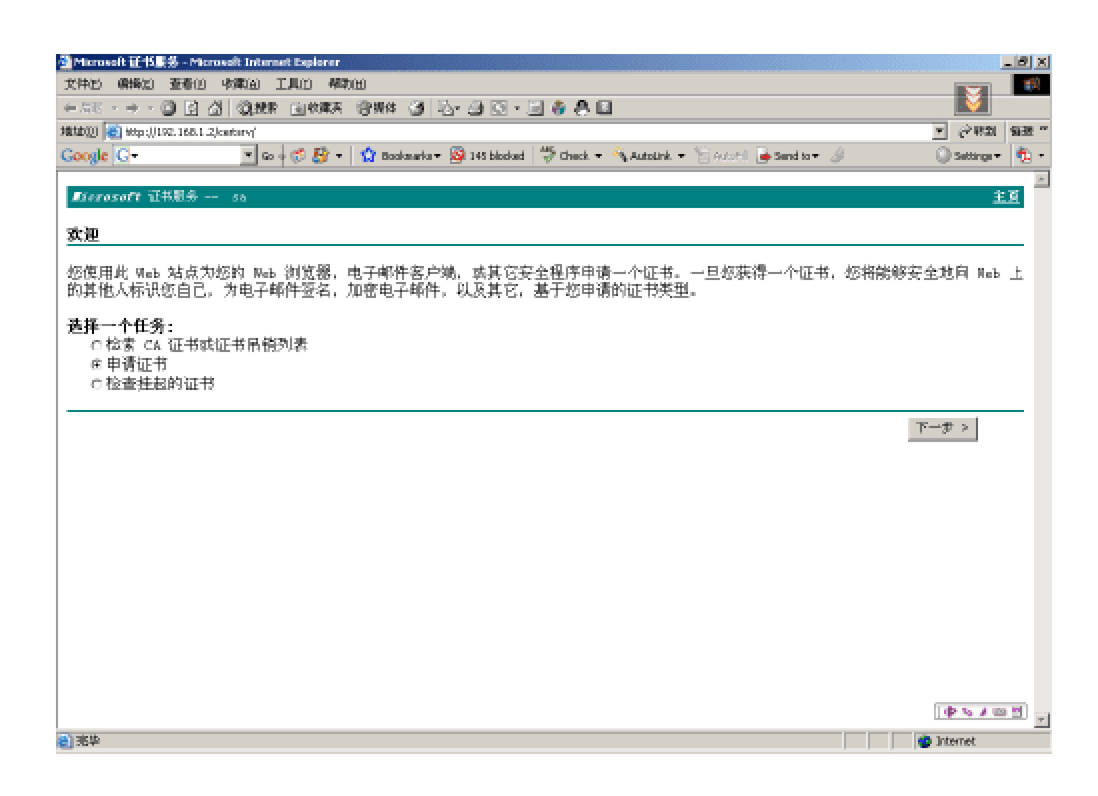


图 7-45　证书服务窗口

7.7　电子政务安全

电子政务是政府机构运用现代信息与通信技术，将管理与服务通过信息化集成，在网络上实现政府组织结构和工作流程的优化重组，超越时间、空间与部门分割的限制，全方位地向社会提供高效、优质、规范、透明的管理与服务。电子政务作为当代信息化最重要的领域之一，已经成为全球关注的焦点，是我国现代化进程中不可缺少的一环，也是我们全面提升政府机构管理与服务水平的重要技术手段。

电子政务的安全问题倍受人们关注，安全性问题是电子政务的首要问题，各国政府都在开展这方面的研究。在电子政务系统的技术选择过程中，应该首先考虑政务信息的安全问题。电子政务系统是供政府和公民使用的信息交流平台，在这之上流动的有可供公用的

信息，还有的是需要保密的非公开信息。即使说一个电子政务网络可以提供强大的功能，可以解决大部分电子政府信息交互的问题，但其本身使用不是本国的软件、硬件，而这些软件、硬件使用的技术不是本国所掌握的或者说这些软硬件并不能保证电子政府免受病毒侵害、黑客攻击，那么，何谈电子政务的安全性，稳定性。这样一来，我们的很多政务信息就不只是“公之于众”了，而且将会是“大白于天下”了！

1．电子政务安全的威胁

电子政务安全是一个复杂的系统工程。仅从安全威胁的来源来看，可以分为内、外两部分。所谓“内”，是指政府机关内部；而“外”，则是指社会环境。来自于外部的威胁有病毒传染、黑客攻击、信息间谍、信息恐怖活动、信息战争、自然灾害等，而来自内部的威胁则包括内部人员恶意破坏、管理人员滥用职权、执行人员操作不当、内部管理疏漏、软硬件缺陷等。

一般说来电子政务安全中普遍存在着以下几种安全隐患。

（1）窃取信息

由于未采用加密措施，调制解调器之间的信息以明文形式传送，入侵者使用相同的调制解调器就可以截获传送的信息。同时，政府机关内部人员更是可以十分轻松地将一些机要信息泄露出去，此谓“监守自盗”。

（2）篡改信息

当入侵者掌握了信息的格式和规律之后，通过各种方式，在原网络的调制解调器之间增加两个相同类型的调制解调器，将通过的数据在中间修改，然后发向另一端。这便严重破坏了原信息的完整性与有效性。

（3）冒名顶替

由于掌握了数据的格式，并可以篡改通过的信息，攻击者可以冒充合法用户及送假冒的信息或者主动获取信息，而远端用户通常很难分辨。同时，由于内部权限分配不明或者滥用他人名义实施违法活动，极有可能造成“栽赃嫁祸”。

（4）恶意破坏

由于攻击者可以接入网络，则可能对网络中的信息进行修改，掌握网上的机要信息，甚至可以潜入两边的网络内部，其后果是非常严重的。如果政府内部人员与外部不法分子勾结或由于发泄私愤，从而破坏重要信息的数据库或其他软硬件，后果更是不堪设想。

（5）失误操作

由于缺乏明确的操作规程和必要的备份措施，加之部分工作人员的安全意识不强和安全技术有限，一旦出现失误操作，重要的信息将无法恢复。

2．电子政务安全的需求

安全的电子政务应该实现五项性能，即有效性、保密性、完整性、可鉴别性和可监控/审查性。

（1）有效性

电子政务作为政务的一种形式，其信息的有效性将直接关系到国家、企业、个人的政治利益、经济利益和声誉。试想，如果政府的灾情、疫情电子公告出现差错，那么，极有可能引发社会动荡。因此，要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，以保证政务信息在确定的时刻、

确定的地点都是有效的。

（2）机密性

电子政务的信息直接代表着国家和企业的机密。例如，很多对外贸易企业的网上“报关”，所传输的信息都是企业的商业秘密，必须保证其机密性。然而，电子政务是建立在一个较为开放的网络环境上的（尤其 Internet 是更为开放的网络），维护机密是电子政务全面推广应用的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取。

（3）完整性

电子政务简化了政务过程，减少了人为的干预，同时也带来维护政务信息的完整、统一的问题，保持政务信息的完整性是电子政务应用的基础。比如统计部门网上采集关系国计民生的数据，如果其完整性得不到保证，信息出现差错，那么，将最终影响政府做出正确的决策，其严重性可想而知。因此，要预防对信息的随意生成、修改和删除，同时要防止数据传送过程中信息的丢失和重复并保证信息传送次序的统一。

（4）可鉴别性

电子政务直接关系企业和个人的利益，如何确定网上管理的行政对象正是所期望的管理对象这一问题则是保证电子政务顺利进行的关键。像税务系统正在实施的“金税工程”，如何确定纳税人的身份，如何确保企业不对网上下达的催税通知加以抵赖，都是十分重要的问题。因此，要在交易信息的传输过程中为参与政务的个人、企业或国家提供可靠的标识。

（5）可监控/审查性

根据机密性和完整性的要求，应对数据审查的结果进行记录。同时，国家正实施为了实现审计工作数字化的“金审工程”，更是需要各政府机关把网上的政务信息加以保留，已备审计。

3．电子政务安全的对策

根据国家信息化领导小组提出的“坚持积极防御、综合防范”的方针，可以从如下三方面解决好我国电子政务的安全问题，即“一个基础（法律制度），两根支柱（技术，管理）”。

信息安全要靠技术，更要靠管理，要把技术和管理相结合，要以人为本，提高安全意识，才能增强信息安全的保障。当然，所有这些都必须建立在国家各种法律制度的基础之上，才会得到切实的保障，如图 7-46 所示。

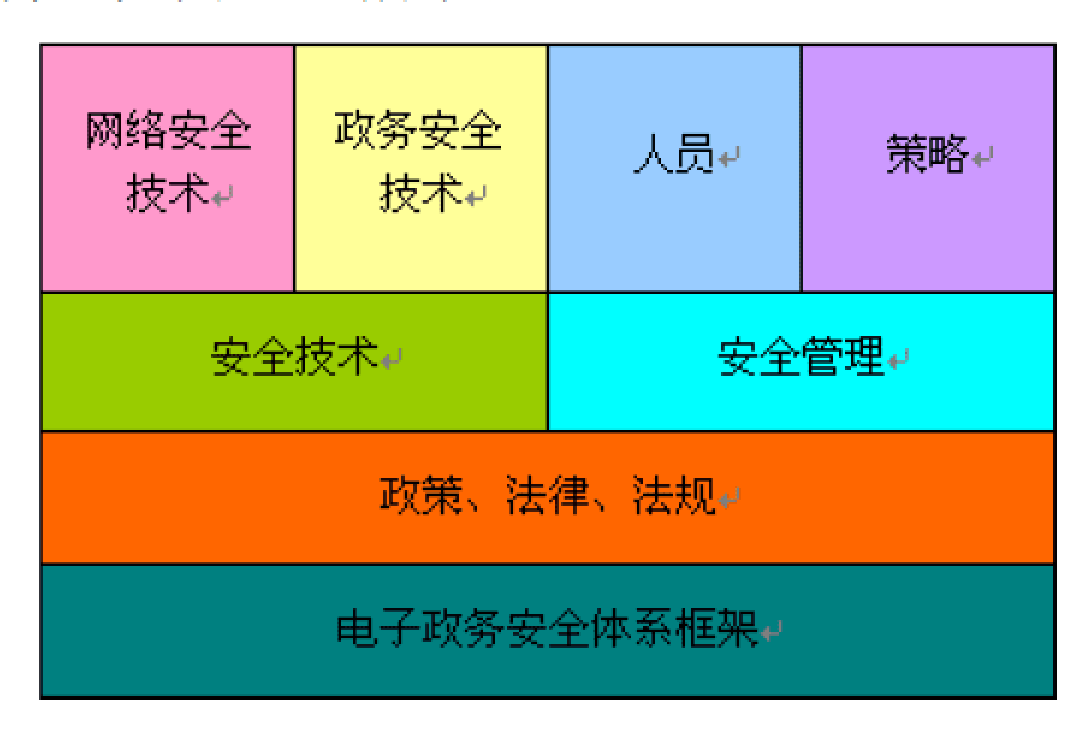


图 7-46　电子政务安全对策

4．网络安全技术

一个全方位的计算机网络安全体系结构包含网络的物理安全、访问控制安全、系统安全、用户安全、信息加密、安全传输和管理安全等。充分利用各种先进的主机安全技术、访问控制技术、防火墙技术、安全审计技术、安全管理技术、系统漏洞检测技术、黑客跟踪技术，在攻击者和受保护的资源间建立多道严密的安全防线，极大地增加了恶意攻击的难度，并增加了审核信息的数量，利用这些审核信息可以跟踪入侵者。

在实施网络安全防范措施时，要做到以下几点。

（1）首先要加强主机本身的安全，做好安全配置，及时安装安全补丁程序，减少漏洞；

（2）其次要用各种系统漏洞检测软件定期对网络系统进行扫描分析，找出隐患，及时修补；

（3）建立完善的访问控制措施，安装防火墙，加强授权管理和认证；

（4）安装防病毒软件，加强内部网的整体防病毒措施；

（5）对敏感的设备和数据要建立必要的物理或逻辑隔离措施；

（6）利用数据存储技术加强数据备份和恢复措施；

（7）建立详细的安全审计日志，以便检测并跟踪入侵攻击等。

5．政务安全技术

我们区别地借鉴电子商务在此方面的成功经验。

（1）加密技术

加密技术是一种主动的信息安全防范措施，可根据需要在信息交换的阶段使用。目前，加密技术分为两类，即对称加密和非对称加密。它可以解决诸如信息的篡改、假冒等问题。

（2）数字签名

通过数字签名能够实现对原始报文的鉴别和不可抵赖性。ISO/IEC JTC1 已在起草有关的国际标准规范。该标准的初步题目是“信息技术安全技术带附件的数字签名方案”，它由概述和基于身份的机制两部分构成。

（3）认证机构（CA）

目前，全方位税收电子化系统的“金税工程”、完整的通关业务电子化的“金关工程”等，都需要实现网上安全支付。因此，建立安全的认证体系（CA）也是电子政务的中心环节，建立 CA 的目的是加强电子证书和密钥的管理工作，控制交易的风险，从而推动电子政务的发展。与电子商务 CA 的情形不同，由于电子政务的一方是政府机构，其本身就是天然的值得信赖的 CA。

（4）安全认证协议

SSL（安全槽层）协议是由 Netscape 公司研究制定的安全协议，该协议向基于 TCP/IP 的客户/服务器应用程序提供了客户端和服务器的鉴别、数据完整性及信息机密性等安全措施。该协议通过在应用程序进行数据交换前交换 SSL 初始握手信息来实现有关安全特性的审查。该协议已成为事实上的工业标准，并被广泛应用于 Internet 和 Intranet 的服务器产品和客户端产品中。

SET 向基于信用卡进行电子化交易的应用提供了实现安全措施的规则。它是由 Visa 国际组织和万事达组织共同制定的一个能保证通过开放网络（包括 Internet）进行安全资金支付的技术标准。SET 1.0 版已经公布并可应用于任何银行支付服务。

6．安全管理方面

在电子政务的安全建设中，管理的作用至关重要。网络提供多种便捷的应用，帮助我们提高工作的效率，而同时因为许多管理上的原因，使我们的网络不安全、不稳定，特别是在电子政务建设过程中网络的安全问题，由于政府工作人员对信息网络安全方面警惕性不高，这样就导致了效率的低下，浪费了投资，严重时会引起泄密事件。

（1）管理对象

重点在于人和策略的管理，人是一切策略的最终执行者。

（2）管理内容

① 核心业务层与外网隔离

党政军内部网络是我国信息网络的重要组成部分，按照 2002 年发过的 17 号文件精神，国务院办公厅把信息网络分为内网(涉密网)、外网(非涉密网)和因特网三类，而且明确内网和外网要物理隔离。但从近几年部分单位安全检查遇到的案例来看，有的不遵守安全保密规定，将内网直接或间接地与因特网连接，这些问题的存在直接带来了安全威胁。

② 政务系统中权限的控制

电子政务需要划分成若干个安全域，不同的安全域中，安全的要求、级别是不一样的，因此需要把使用不同级别政务信息资源的用户划分成不同类型，实现不同类型人员对不同级别信息访问的控制策略。

③ 系统的安全备份与恢复机制

鉴于政务信息的重要性和特殊性，建立必要的备份制度和有效的系统和数据恢复机制是保障电子政务安全的基本需求。

④ 定期检测和审计机制

对于电子政务系统运行中的漏洞以及工作人员在执行安全策略方面的疏忽必须加以监控并且及时纠正。

⑤ 信息发布严格合理审查机制

政府信息化的要求之一就是利用互联网络做强有力的宣传，同时从安全的角度，还需要防止敌对力量通过网络系统散布不满情绪、制造流言、做颠覆性的宣传等不利于政治与社会稳定的行为。因此，需要对发布的信息进行必要的审查，尤其是要看管好 BBS 系统。

⑥ 废旧信息存储介质的处理

有关专家特别要强调利用废旧磁媒体获取信息的问题。旧的计算机、旧的磁盘、磁带、光盘等，往往存储过涉密信息，有的国家可以从消过磁的介质中恢复曾经存储过的信息，情报机关就利用收集废旧物品的机会专门搜集废旧磁媒体，从中获取情报。因此对废旧磁媒体要特别加强管理。

（3）管理步骤

① 事前明确要求

② 事中严格监督

③ 事后严肃惩处

7．安全法律方面

（1）现有部分计算机网络管制法：

①《中华人民共和国保守国家秘密法》第三章

②《计算机病毒控制规定》

③《计算机软件保护条例》

④《中华人民共和国计算机信息系统安全保护条例》

⑤《中华人民共和国计算机网络国际联网管理暂行规定》

⑥《中华人民共和国计算机信息网络国际联网管理暂行规定实施细则》

（2）现有部分主要行政法：

①《中华人民共和国行政许可法》

②《中华人民共和国行政诉讼法》

③《中华人民共和国行政复议法》

④《中华人民共和国行政处罚法》

⑤《中华人民共和国行政监察法》

（3）有关部委制定的规章制度，比如《国土资源管理系统行政为民措施》和《国土资源管理系统工作人员禁令》都是比较有效的保障网上政务安全运行的成功典范。

（4）电子政务的安全实施和保障，应以国家法规形式将其固化，成为电子政务实施和运行的行为准则，成为电子政务国际交往的重要依据。因此，制订政务信息公开法，适度的解密和规范开放的规则，保护政府部门间信息的正常交流。建立电子签章（含数字签名和电子印章）和电子文档的立法保护。加快个人数据保护法的制订是必要的。

8．电子政务安全的特别注意问题

（1）电子政务产品的自主开发性

由于电子政务的国家涉密性，电子政务系统工程的安全保障需要各种有自主知识产权的信息安全技术和产品，全面推动自主研发和创新这些技术与产品是电子政务安全的需要。

电子政务安全涉及信息安全产品的全局配套和科学的布置，产品选择应考虑产品的自主权和自控权。产品涉及到安全的操作系统、安全的硬件平台、安全的数据库、强认证设施等。

（2）政务公开与信息安全“度”的把握

在加强信息公开的同时，不能忽视信息安全。信息安全是中央反复强调的非常重要的问题。电子政务建设涉及政务管理的核心业务，涉及国计民生和国家安全。因此，我们要增强安全意识，严格执行国家和部颁布的安全和保密规定，建立严格的信息公开审查制度。同时，要采取切实的技术手段，积极防御各类黑客行为、计算机病毒等对电子政务系统所构成的威胁。也就是说，要以辩证的眼光看待信息公开和安全问题，正确处理好两者之间的关系，既不能为了公开而忽视安全，也不能将安全问题绝对化，阻碍信息公开和应用发展。要通过制度建设，形成安全与应用相互促进的良性发展机制。

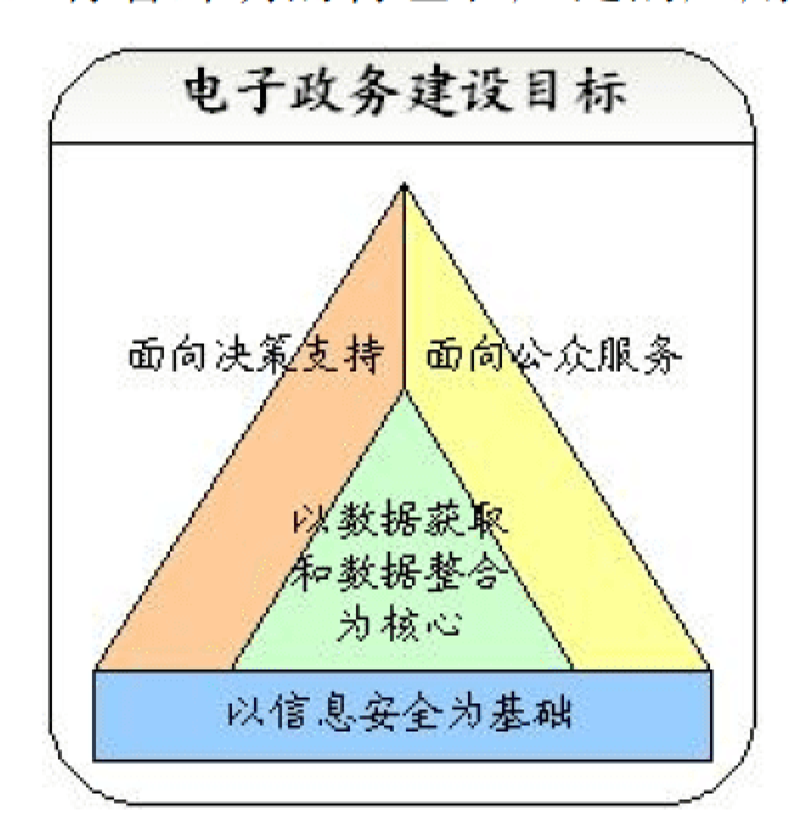
（3）强化安全观念的宣传，重视工作人员的培训与教育

安全产品的配置虽然可以降低安全风险，但不能完全消除安全风险。安全产品靠人来操作、使用、管理，人员的安全意识、安全素质显得十分重要。必须加强信息安全人才队伍的建设，提高工作人员信息安全的意识，从而使各种安全策略和措施得以切实的实现。

无论任何形式的政务，安全都是最基本的要求。如果连安全都没有保证，再先进的技术，再方便的功能，人们也只能敬而远之。只有切实做好安全工作，解决好安全问题，才能真正做到“一网管天下”，电子政务时代才会真正到来！

9．电子政务安全应用整体解决方案

整体解决方案以实现电子政务建设目标和满足客户业务需求为导向，以信息安全保障为基础，在统一的安全电子政务平台、国家电子政务标准、信息技术国际主流技术标准和电子政务业务经验积累的基础之上构建。如图 7-47 所示。平台采用先进的技术路线和成熟的技术架构，有着鲜明的特色和广泛的应用。



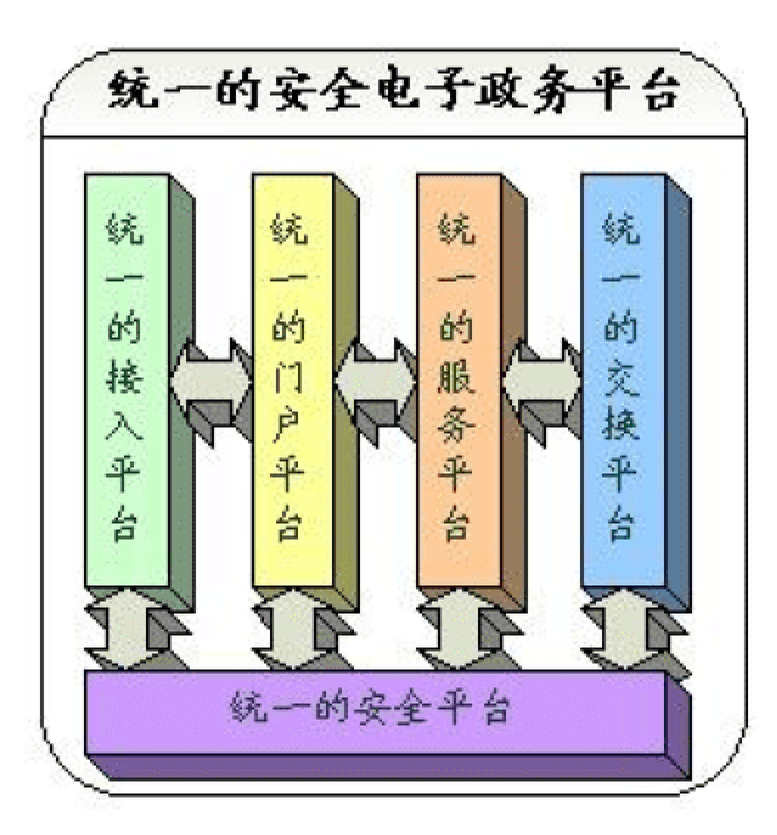


图 7-47　电子政务统一安全平台

（1）技术体系

① 支持多层应用体系结构，客户端应用和浏览器应用相结合与服务器进行交互。

② 支持 J2EE，.Net 等应用技术架构，支持 EJB，CORBA，COM+等组件技术。

③ 支持使用 XML（XMLSechma，XSLT，XForm）进行数据交换、数据验证、元数据的存储等。

④ 支持面向服务的应用架构（SOA），支持 SOAP，WSDL，UDDI。

⑤ 支持基于 PKI 的信任服务体系和基于 PMI 的授权服务体系，支持单点登录（SSO）、数字签名和数据加密。

⑥ 能够支持系统应用集成。

如图 7-48 和图 7-49 所示。

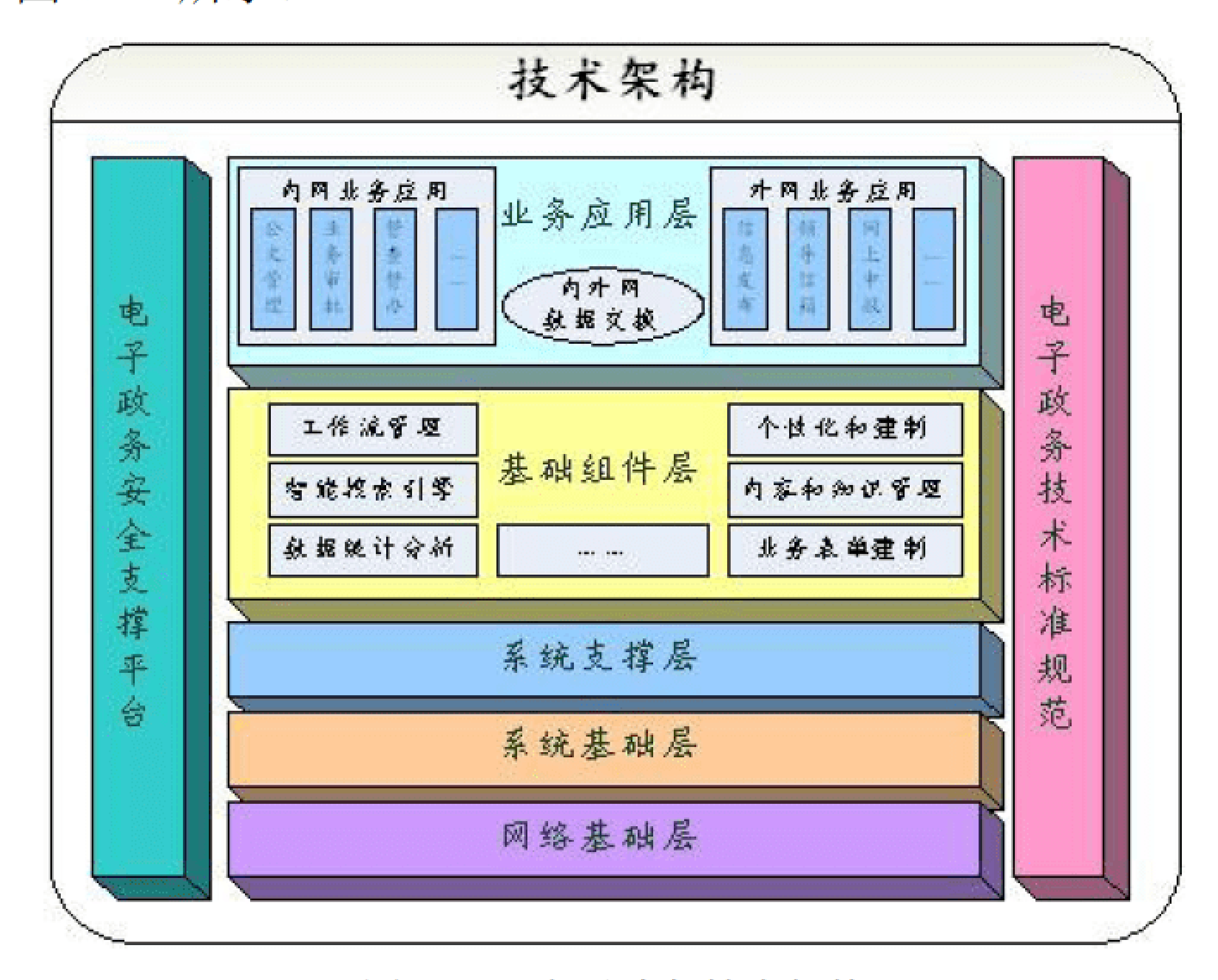


图 7-48　电子政务技术架构

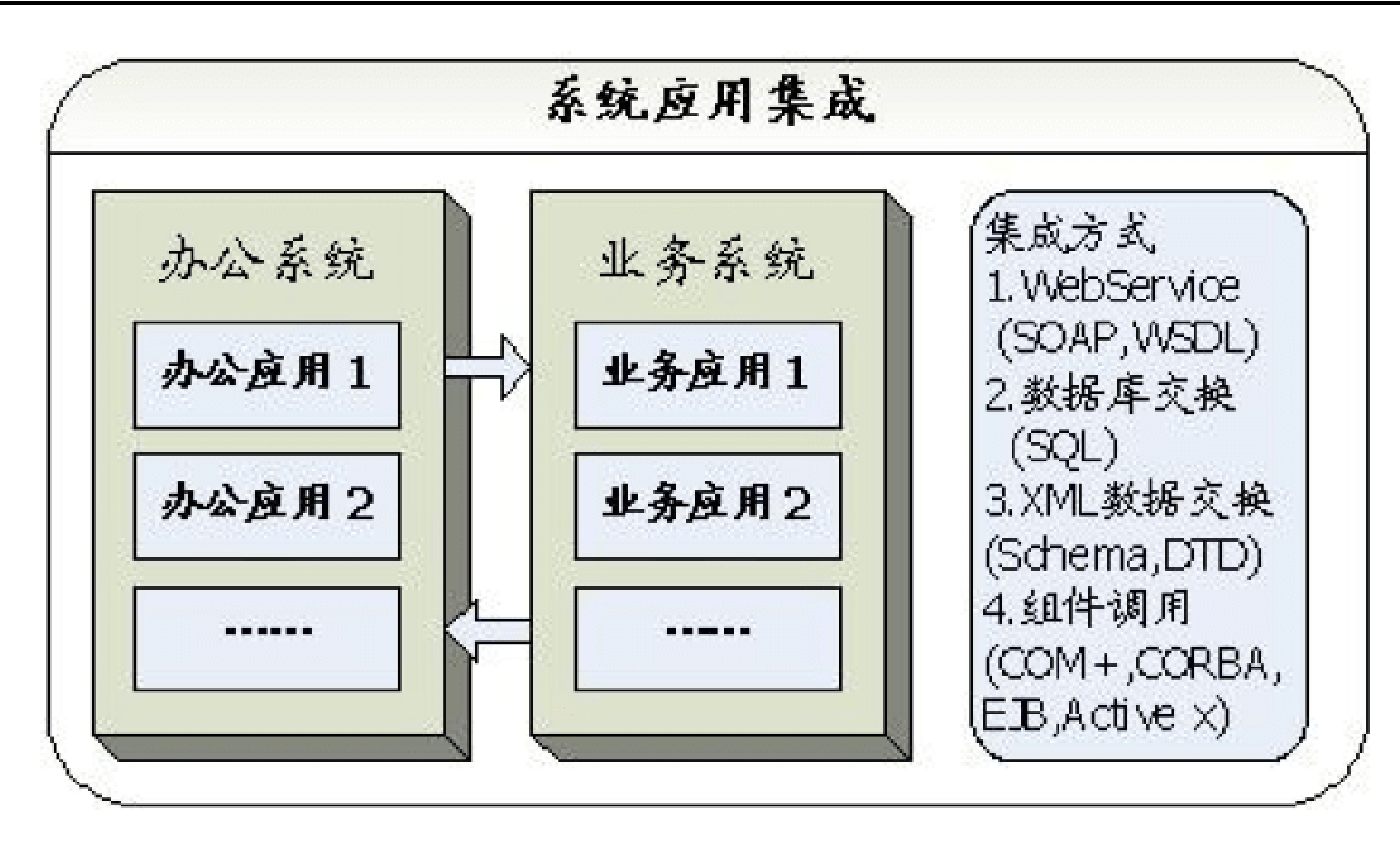


图 7-49 电子政务系统应用集成

（2）方案特色

① 方案的产品平台提供通用的组件支持，能够减少重复开发工作，保证产品和项目的质量，缩短应用系统的开发周期，有利于系统的扩展。

② 方案充分考虑了各种业务需求有机结合，既能实现通用的办公业务功能，又能满足特定的行业业务应用，还可以完成内外网的数据交换、信息共享、数据挖掘等功能。

③ 方案中信息安全与电子政务业务应用的紧密结合，充分利用基于 PKI 的信任服务体系和密码安全服务平台，保证业务数据和业务流程的安全。

④ 结合多年的电子政务领域和信息安全领域的经验，我们还可以在为客户提供解决方案的同时，提供有关电子政务业务管理和安全保障体系的有益建议。

⑤ 方案和产品的架构紧密跟踪国家电子政务标准和国际主流技术标准，开放性好，便于系统的升级维护，以及与各种政务信息系统进行集成。

⑥ 结合我们成熟的方案、稳定的产品和丰富的经验，我们可以为党政机关客户进行信息化规划和信息技术咨询，帮助客户集成现有的各种系统。

习题

1. 简述互联网企业应用包括哪些内容。
2. 简述互联网政府应用包括哪些内容。
3. 理解互联网面临哪些安全威胁。
4. 简述电子商务安全包括哪些内容。
5. 简述电子政务包括哪些内容。

第 8 章　网络安全规划

教学提示

在企业内建立一个统一规划、合理布局、协调发展、安全畅通的、具有高度安全的信息网络，在此基础上，以应用系统的建设和整合为主轴，通过不断的努力，建成一套安全、实用、可扩展的网络系统，建设各项信息基础设施实现企业各级领导、各部门之间的电子公文交换、秘密文件传输、信息资源共享、业务数据访问处理等广泛的信息应用，更好地为各级领导和各部门提供办公、决策和信息服务，是企业信息化的必然要求。

网络信息安全问题是一个系统的、复杂的、长期的问题，有效解决网络信息安全问题开始于合理的网络安全规划。网络安全规划包括网络安全现状分析、体系框架结构、体系层次、设计原则、网络安全攻击、安全机制、安全技术、安全措施、安全服务等。

通过对本章的学习，应当充分掌握网络信息安全规划的相关内容，能够针对具体的计算机网络提出适当的安全规划，全面分析计算机网络所面临的各种安全问题，并根据这些安全问题提出合理、有效的解决方案。

教学重点

- 网络安全现状分析和需求分析。
- 网络安全规划框架体系结构。
- 网络安全设计原则。
- 网络安全技术。

8.1　网络和应用现状分析

要解决网络信息安全问题，首先要做的就是对网络和应用的现状进行分析，找出网络和应用对安全的需求，并针对这些安全需求进行网络安全规划，只有满足网络实际情况的网络安全规划才是有意义的。

8.1.1　网络中存在的安全威胁

网络系统的安全性和可靠性成为广大网络系统受益者共同关注的焦点。而网络自身的一些特点，在为网络系统用户带来发展机遇的同时，也带来了巨大的风险。网络安全威胁主要存在于以下几个方面。

（1）网络的共享性

资源共享是建立计算机网络的基本目的之一，但是这也为系统安全的攻击者利用共享的资源进行破坏活动提供了机会。

（2）网络的开放性

网上的任何用户很容易浏览到一个企业、单位，以及个人的敏感性信息。受害用户甚

至自己的敏感性信息已被他人盗用却全然不知。

（3）系统的复杂性

计算机网络系统的复杂性使得网络的安全管理更加困难。

（4）边界的不确定性

网络的可扩展性同时也必然导致了网络边界的不确定性。网络资源共享访问时的网络安全边界被破坏，导致对网络安全构成严重的威胁。

（5）路径的不确定性

从用户宿主机到另一个宿主机可能存在多条路径。一份报文在从发送节点达到目标节点之前可能要经过若干个中间节点。所以起点节点和目标节点的安全保密性能并不能保证中间节点的不可靠性问题。

（6）信息的高度聚集性

当信息分离的小块出现时，信息的价值往往不大。只有将大量相关信息聚集在一起时，方可显示出其重要价值。网络中聚集了大量的信息，特别是 Internet 中，它们很容易遭到分析性攻击。

总之，网络系统为广大用户带来方便的同时，也带来了安全隐患，我们必须对这些安全隐患进行有效的解决，否则，一旦发生重大安全问题，网络用户将得不偿失。

8.1.2 网络现状分析

网络安全问题是一系列复杂的问题，涉及到网络的多个方面，所以网络现状分析是网络安全规划的第一步。只有了解了网络的各种具体情况，才能有针对性地提出切实可行的安全解决方案。网络现状分析包括如下内容。

（1）网络规模。具体包括服务器的配置规格（如品牌、型号、运算速度、存储容量等）以及对应的数量、普通计算机的配置规格以及对应的数量、各种网络设备（如交换机、路由器以及网卡等）的配置规格以及对应的数量。

（2）网络结构。即计算机和计算机、计算机和网络设备、网络设备和网络设备之间的连接方式，合理的网络结构有利于管理，减少管理人员的工作量，提高网络的灵活性。

（3）网络跨度。即网络的物理范围的大小，比如是几十米、几百米还是几千米或者更大范围，是否使用 VPN 来实现远距离的连接。

（4）是否连接互联网。对于和互联网物理隔离的网络系统，可以不用防火墙；对于直接连接到互联网的网络系统，防火墙是网络安全的一项非常重要的安全措施。

（5）网络速度。整个网络系统是百兆网还是千兆网，对于网络速度的了解，有利于选择合适的网络安全产品与之适应，这对于安全解决方案的制作以及网络应用都是非常重要的。

（6）系统平台。计算机的操作系统平台提供了一定的安全保障，不同的系统提供的安全保障内容相差较大，所以对系统平台的了解，有利于针对系统平台的安全问题提供适当的解决方案。

对于网络现状了解得越清楚，就越能够准确地发现系统中存在的安全隐患，最后提出的解决方案就越有针对性，即能够防止因为滥用安全措施导致费用过高，又能够有效提高整个网络系统的安全性。

8.1.3　应用现状分析

应用现状分析是指对建立在企业网络基础上的应用情况的分析。企业信息化以后，计算机为企业提供了各种各样的满足企业需要的应用，这些应用在给企业带来效率和效益的同时，也带来了一定的安全隐患，对这些应用的分析，有利于充分利用其带来的利益的同时，防止和避免相关的安全问题。应用现状分析主要包括如下内容。

（1）是否通过互联网对外提供 Web 服务，如果是的话，就需要对 Web 服务器的安全进行特殊处理，比如安装防火墙、网页防篡改、与内部重要网络进行物理隔离以及采取其他防止被攻击和破坏的安全措施。

（2）是否通过文件服务器共享文件，如果是的话，就需要对文件服务器上的共享目录做具体的权限设置，防止有人越权查看、修改、复制、删除文件服务器上的文件，这项措施对于防止内部人员泄密具有非常重要的意义。

（3）是否存在跨互联网的应用系统，如果存在的话，为了应用系统的安全运行，需要采取 VPN 技术作为网络直接的连接方式，而不是直接将数据在互联网上进行传输，这对于企业的重要应用非常重要，因为系统数据被窃取、篡改、丢失都将对企业造成不同程度的损失。

（4）网络中是否存在重要信息资料从内部网络泄密的可能，如果是的话，就需要部署对这些文件资料的保护措施，特别是对内部人员的行为进行管理，比如禁止随意使用便携式存储设备在内部网络中复制文件，禁止随意使用打印机打印文件，禁止使用刻录机刻录文件等，实施内网安全管理可以在某种程度上有效解决内网安全问题。

（5）网络中是否存在通过互联网泄密的可能，如果可能的话，就需要对员工在互联网上的行为进行控制，比如禁止随意发送邮件，禁止通过互联网外传企业内部文件资料，禁止使用聊天工具向外泄露企业内部的重要信息。

（6）网络中是否存在引入计算机病毒的地方（比如从外部复制光盘内容到企业内部），如果存在的话，对这些地方需要严格管理，为了防止意外情况的发生，还需要对企业内部计算机均安装杀毒软件，防止网络中一台计算机感染病毒以后，蔓延到整个网络，从而导致网络系统的损失。

计算机网络虽然为企业提供了丰富多样的应用，但是不同企业在使用本企业计算机网络所提供的应用是有所不同，只有针对具体网络提供的企业应用进行详细、全面的分析，才能发现其中存在的安全隐患，找出对应的解决方案，为企业信息化提供安全保障。

8.1.4　安全系统设计目标

安全系统设计的目标就是要全方位地、分层次地解决网络安全问题，不同层次反映了不同的安全问题，我们把网络安全问题分为 5 个层次，它们分别是物理层安全问题、系统层安全问题、网络层安全问题、应用层安全问题和安全管理问题。

（1）物理环境的安全性（物理层安全问题）

该层次的安全包括通信线路的安全、物理设备的安全和机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网管软件、传输介质），软硬件设备安全性（替换设备、拆卸设备、增加设备），设备的备份，防灾害能力、防干扰能力，设备的运行环

境（温度、湿度、烟尘），不间断电源保障，等等。

（2）操作系统的安全性（系统层安全问题）

该层次的安全问题来自网络内使用的操作系统的安全，如 Windows NT，Windows 2000 等。主要表现在三方面，一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等。二是对操作系统的安全配置问题。三是病毒对操作系统的威胁。

（3）网络的安全性（网络层安全问题）

该层次的安全问题主要体现在网络方面的安全性，包括：网络层身份认证，网络资源的访问控制，数据传输的保密与完整性，远程接入的安全，域名系统的安全，路由系统的安全，入侵检测的手段，网络设施防病毒等。

（4）应用的安全性（应用层安全问题）

该层次的安全问题主要由提供服务所采用的应用软件和数据的安全性产生，包括 Web 服务、电子邮件系统、DNS 等。此外，还包括病毒对系统的威胁。

（5）管理的安全性（管理层安全问题）

安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其他层次的安全漏洞。

8.2 网络安全系统整体规划

网络安全系统的整体规划，应在科学的安全体系框架的指导下，在详细的系统功能、网络结构和安全风险分析的基础上，逐步摸清各个系统的安全需求，划分出不同的安全子系统，在不同层次采取不同的安全措施，选用合理的安全产品，通过各种网络安全技术和机制的综合运用，加以实现。

（1）安全第一原则

这有两层含义，一是在观念上把网络安全作为一项重点工作贯穿企业综合信息网建设的始终，避免“只搭网，无安全；修了路，不敢跑车”的局面，避免由于一开始没考虑安全而在以后以加倍的代价弥补安全缺陷；其次，就是在安全产品选型时，尽量选用具有自主知识产权并通过国家权威监管和测评机构认证的安全产品，避免国外产品的加密强度限制和技术陷阱、安全后门、软件炸弹等。

（2）以人为本，预防和管理为主，安全技术和设施为辅

据统计，95%的网络和信息安全事件均源于网络不设防、安全策略的不得当和内部管理人员的疏忽。因此，在网络安全设计时，一定要把网络安全管理放在首位，使网络安全技术服务于网络安全管理，同时要通过教育培训加强用户的安全意识和安全素质，加强安全管理和防范。

（3）体系化设计原则

安全涉及到方方面面的问题，必须通过建立科学的安全体系框架，才能分析出企业网络在各个层次的不同安全风险和安全需求，并有针对性地采取有力的措施，保证企业网络以及在其上运行的应用系统和数据的安全。

（4）全局性、综合性、均衡性原则

从全局出发，综合考虑各种安全风险，采取相应的安全措施，并根据风险的大小，采取不同强度的安全措施，一方面保证了企业网络的各种安全需求得到了解决，另一方面，在必要的冗余基础上，采取最简单的安全措施，提供具有最优的性能价格比的安全解决方案。

（5）可行性、可靠性、安全性原则

在采用安全系统之后，不会对原有的网络和应用系统有大的影响。在保证网络和应用系统正常运转的前提下，保证系统的安全。同时安全系统应该是可实施的，选用的安全产品是技术成熟、经过实际检验的安全可靠的产品。

（6）分步实施原则：分级管理，分步实施。

由于网络系统及其应用扩展范围广阔，随着网络规模的扩大及应用的增加，网络脆弱性也会不断增加。一劳永逸地解决网络安全问题是不现实的。同时由于实施信息安全措施需要相当的费用支出。因此分步实施，既可满足网络系统及信息安全的基本需求，也可节省费用开支。

8.2.1　安全体系框架分析

安全方案的科学性、可行性是其可顺利实施的保障。安全方案必须架构在科学的安全体系和安全框架之上，因为安全体系框架是安全方案设计和分析的基础。

为了系统、科学地分析安全方案涉及的各种安全问题，在大量调查研究的基础上，我们提出了下面的安全体系框架，它反映了信息系统安全需求和体系结构的共性。具体说明如下。

安全体系框架是一个三维结构：

第一维（X 轴）是安全服务特性，给出了 7 种安全属性；

第二维（Y 轴）是系统单元，给出了信息网络系统的组成；

第三维（Z 轴）是协议层次，给出了国际标准化组织 ISO 的开放系统互连（OSI）模型。

安全体系框架的具体模型和介绍如图 8-1 所示。

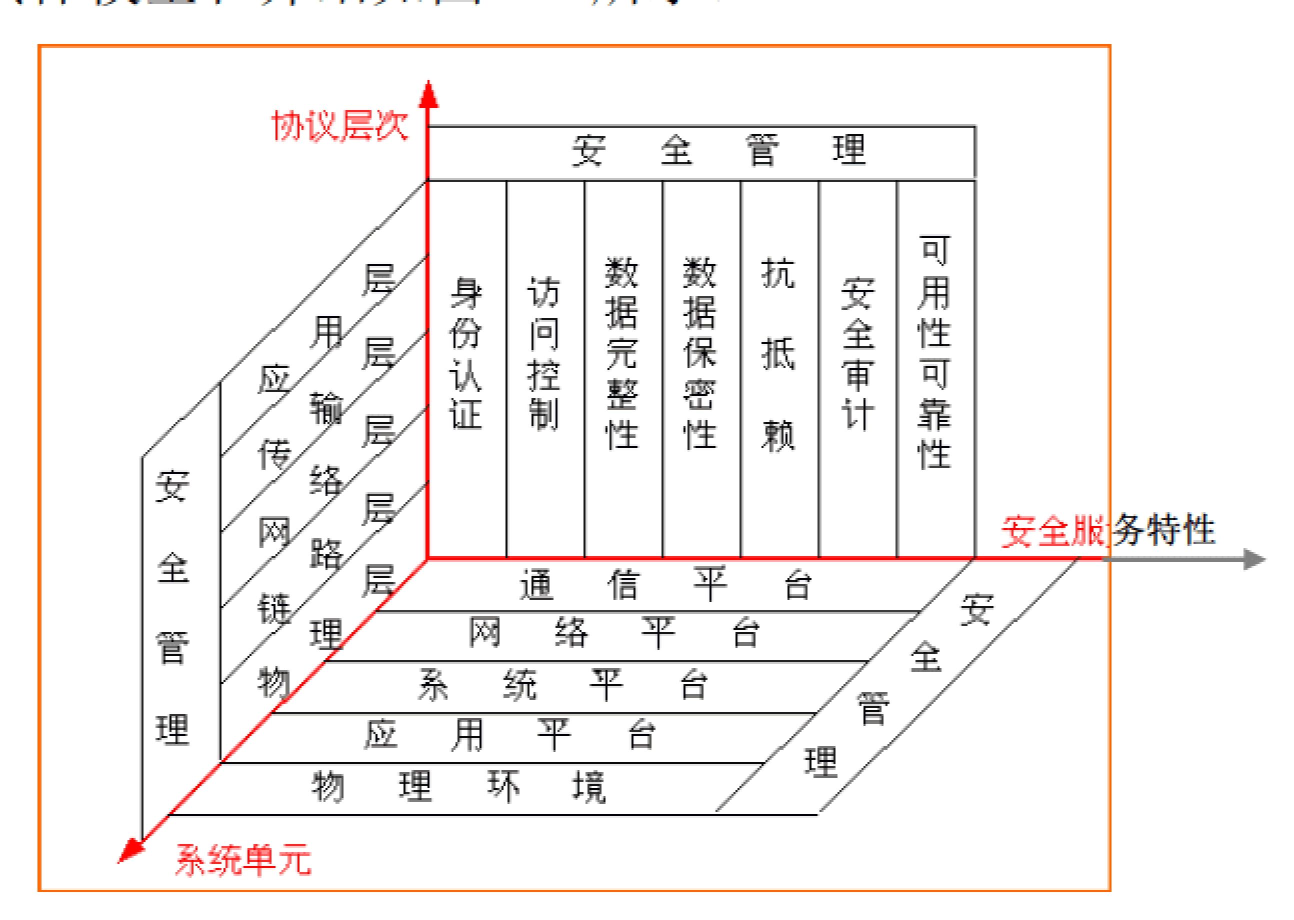


图 8-1　安全体系框架

1. 安全服务维

安全服务源于 ISO7498-2，并做了适当扩展。它列举了信息网络系统中涉及到的 7 种主要安全服务，具体如下：

（1）身份认证，用于确认所声明的身份的有效性；

（2）访问控制，防止非授权使用资源或以非授权的方式使用资源；

（3）数据保密，数据存储和传输时加密，防止数据窃取、窃听；

（4）数据完整，防止数据篡改；

（5）不可抵赖，取两种形式中的一种，用于防止发送者企图否认曾经发送过数据或其内容和用以防止接收者对所收到数据或内容的抗否认；

（6）审计管理，设置审计记录措施，分析审计记录；

（7）可用性、可靠性，在系统降级或受到破坏时能使系统继续完成其功能，使得在不利的条件下尽可能少地受到侵害者的破坏。

2. 协议层次维

协议层次维由 ISO/OSI 参考模型的七层构成，用于分析在不同协议层次的安全需求。与 TCP/IP 层次对应，可以把会话层、表示层、应用层统一为“应用层”。

3. 系统单元维

系统单元维描述了信息网络的各个组成成分，是协议层次的投影。

（1）通信平台，信息网络的通信平台；

（2）网络平台，信息网络的网络系统；

（3）系统平台，信息网络的操作系统平台；

（4）应用平台，信息网络各种应用的开发、运行平台；

（5）物理环境，信息网络运行的物理环境及人员管理。

4. 安全管理

贯穿于上述三个方面，各个层次的是安全管理。通过技术手段和行政管理手段，安全管理将涉及到各系统单元在各个协议层次提供的各种安全服务。

安全管理的核心内容包括：

（1）确定安全管理的范围和职责：根据不同层次的安全需求和应用模式，在不同平台确定不同的安全域（一个明确的“用户－资源－授权”的安全管理范围），在每个安全域内指定一个安全管理员或安全管理小组，明确其安全管理的用户和资源对象（包括网络设备、服务器和应用系统），确定其安全管理的权力和责任。

（2）在安全域内，遵循统一的安全策略和安全管理原则，制定相应的安全管理制度，采用相应的安全技术，配置合适的安全产品，对企业网络和应用进行管理。

利用上述安全体系框架，我们就可以比较全面地对一个网络系统存在的各种安全需求进行分析。比如，对于系统单元维的网络平台，其安全需求主要集中在网络节点之间的互相认证和访问控制，以及网络系统的可用性和可靠性方面；而对于应用平台，则可能会涉及到安全服务中的所有安全服务。

在安全方案设计中，首先要确定安全方案所涉及到的系统单元，其次要考虑该系统单元在各个层次所提供的安全服务（功能），最后还应考虑这些单元系统之间的逻辑关系，在整体安全体系框架下，划分成不同的安全子系统，分别提供相应的安全解决方案，才能

提供全面的、合理的、有机的安全服务。

8.2.2　安全子系统划分

利用上面的安全体系框架，我们可以把一般的信息网络安全系统划分为以下几个安全子系统。

（1）通信平台安全子系统。主要对数据在广域网传输时提供安全保障，在安全体系框架中涉及到数据完整性和保密性、链路可用性和可靠性等安全服务，一般采用链路加密设备、冗余链路等措施；

（2）网络平台安全子系统。主要需要提供安全的网络拓扑，防范来自外部网络的安全威胁，尽早发现安全隐患和安全事件，把它们控制在一个比较小的网络范围内。在安全体系框架中，网络安全子系统涉及到网络节点间的认证和访问控制、网络可用性和可靠性等服务，一般通过网络拓扑划分，采用防火墙、安全路由器、安全漏洞扫描和实时入侵检测、网络防病毒等软件或设备及其冗余措施实现；

（3）系统平台安全子系统。主要对主机（包括服务器和单机，主要针对关键服务器）进行保护，保证主机上的操作系统和数据的安全。在安全体系框架中，主机安全子系统涉及到用户认证、访问控制、主机上存储的数据的完整性和保密性、访问的审计、主机及其上的服务的可用性和可靠性等安全服务，一般采用增强操作系统安全、主机安全扫描、主机入侵检测、主机防病毒、文件存储加密、数据库存储加密等措施；

（4）应用平台安全子系统。主要为网络应用提供各种安全服务，保证应用系统中使用到的各种数据（如各种公文、人事、财务等信息）的安全。应用安全子系统涉及到在安全体系框架中提及的各种安全服务，如对应用系统的用户认证、访问控制、数据的完整性和保密性、抗抵赖、审计及应用系统的可用性和可靠性，因此这是最复杂的一个安全子系统，可以采用的安全措施有：使用应用开发平台提供的各种安全服务，在应用系统中开发各种安全服务，使用第三方应用安全平台提供的安全服务等。

对企业网络，同样可以划分成上述几个安全子系统。但是由于具体的企业网络有其特殊的网络环境和应用环境，各个安全子系统的侧重点要结合实际需求具体分析。下面我们将针对不同的安全子系统，根据其安全需求，提出我们的安全建议。

8.3　通信平台安全子系统

通信平台安全子系统的目标主要是从通信链路和设备上保证数据传输的安全可靠。它主要对数据在网络硬件设备上传输时提供安全保障。

在企业网络中，网络硬件设备主要包括：

（1）用于连接计算机和计算机、计算机和网络设备以及网络设备和网络设备的网线。

（2）用于使计算机具有通信功能的网卡。

（3）用于建立网络系统的网络设备，包括集线器、交换机、路由器等。

（4）用于为网络系统提供服务的服务器。

（5）用于为网络系统提供安全保障的安全设备，包括硬件 VPN、硬件防火墙等。

这些建立计算机网络的硬件设备为企业网络搭建了一个通信平台，这个平台的安全运行是计算机网络安全的一个基础和前提。只有硬件设备的安全得到保障，整个网络系统的安全才成为可能，可见确保网络通信平台安全子系统的稳定、高效、安全地运行是整个网络系统安全的一个重要组成部分。

8.4 网络平台安全子系统

在安全体系框架中，网络安全子系统涉及到网络节点间的认证和访问控制、网络可用性和可靠性等服务，一般通过网络拓扑划分，采用防火墙、安全路由器、安全漏洞扫描和实时入侵检测、网络防病毒等软件或设备及其冗余措施实现。

8.4.1 网络平台安全域划分

网络平台安全子系统的目标是保证网络边界的安全，确保用户只能访问到授权的网段、服务器和服务。

企业网络除了实现为企业内部信息化以外，为了方便地从互联网上获取相关信息，通常会将企业网络的一部分同互联网连接，在带来网络访问方便的同时，也带来了安全风险，所以需要对连接到互联网的网络边界的安全进行有效的管理。

除了直接连接到互联网上的网络存在边界安全问题，同时各个部门的网络连接同样存在着网络边界安全问题，比如企业总部和各级分支机构之间。

因此，在企业网中，网络平台安全子系统主要是针对各单位局域网的边界安全，可以把每个单位的局域网划分为一个独立的安全域。

8.4.2 网络平台安全需求分析

网络平台的安全需求主要是防范不同网段之间的攻击和非法访问。在企业网络当中，针对总部局域网，网络平台的安全需求主要有以下几点。

（1）重点保护企业网络中的各种应用服务器和数据库服务器，特别是要保证数据库服务器的绝对安全，不能允许任何用户直接访问。对应用服务器，则要保证用户的访问是受到控制的，要能够限制可以访问该应用服务器的用户范围，控制用户只能够通过指定的方式进行访问。

（2）要区分来自省级分支机构的用户和来自其他单位（地市级分支机构、营业网点）的用户，不能允许其他单位的用户直接访问总部的办公网络。

（3）企业网络中重要网段应该与互联网物理隔离，防止来自互联网的攻击造成企业内部重要网段的破坏。对总部网络与各分支机构网络的连接，同样需要注意由此而引起的安全风险，因为这样的攻击可能来自外部，也可能来自企业内部的各个分支机构。因此，要能够及时发现各种可能的网络攻击，特别是针对总部应用服务器的攻击。

上述安全需求，需要通过划分出安全的网络拓扑结构，并通过 VLAN 划分、安全路由器配置和防火墙网关的配置来控制不同网段之间的访问控制，同时，可以采用入侵检测系统来防范各种常见的网络攻击。

8.4.3 安全网络拓扑结构

划分安全网络拓扑的目的是在保证网络应用的可用性的基础上，对网络中的各种服务器提供最大的安全保证。

我们建议采用一种非军事化区（DMZ）的三网段网络结构。

目前网络应用中最通用的一种应用模式是三层结构：用户界面层－应用服务器层－数据库层。应用系统的所有重要数据都存放在数据库层中，用户界面层和应用服务器层只存放一些临时数据。用户通过用户界面层访问应用服务器层，再通过应用服务器访问后面的数据库。在任何时候，都不允许用户直接访问数据库层中的数据库服务器。B/W/D 模式（浏览器/Web 服务器/数据库服务器）的应用是这种三层结构应用的典型，这种模式中客户端使用的是普通的浏览器，Web 服务器可以使用各种主流服务器，后台数据库也可以是任何一种关系型数据库。

根据这种应用模式，使用非军事化区结构的网络拓扑是一种很自然的提高安全性的措施。我们可以采用防火墙来划分这种安全网络拓扑。在防火墙上安装三块网卡，分别连接三个不同网段，即外网（非安全区）、非军事化区和内网（安全区）。

外部用户位于外网，只能够访问到非军事化区，不能访问内网。

内网放置数据库层的各种服务器，存放重要的数据，不允许从外网直接访问。

非军事化放置应用服务器层的各种应用服务器，在目前流行的 B/W/D(浏览器/WEB 服务器/数据库服务器）应用模式中，对应的是各种 WEB 服务器。

位于外网的用户通过用户界面层软件，访问应用服务器；应用服务器再通过特定应用服务访问位于内网的数据库层服务器。

在一个部门内部，可以通过虚网的划分，把安全内网划分成几个子网：数据库服务器子网、内部应用服务器子网、内部用户子网，只限内部用户访问的应用服务器放在内部应用服务器子网。通过虚网的划分，使内部用户子网用户只能访问外网、非军事化区网段和内部应用服务器子网，不能访问数据库服务器子网。

在企业网络中，针对总部局域网，其外网包括各级分子机构的网络用户，他们与总部的网络连接都必须通过防火墙。

8.4.4 防火墙配置方案

防火墙是网络平台的基本安全保证措施，主要用于保护局域网的边界安全，实现不同网段之间的网络层访问控制。下面将首先介绍总部局域网防火墙的配置。

8.4.5 总部局域网防火墙配置方案

总部局域网的防火墙主要用于限制来自省级分支机构、地市级分支机构以及营业网点的用户访问。

我们在总部的中心交换机上，设置一个防火墙网关。该防火墙网关配置三块网卡，把总部网络划分为三个网段。

安全内网：放置企业综合信息系统的数据库服务器，这些数据库服务器只允许应用服务器访问，绝不允许用户直接访问；此外，防火墙的管理工作站也可以放置在安全内网中。

非军事化区：放置企业综合信息系统的应用服务器，包括企业内网中的 WEB 应用服

务器、电子邮件服务器、DNS 服务器等。这些服务器可以允许用户访问，但是其访问是受到防火墙网关控制的，如只允许通过电子邮件服务器发送、接收邮件，只允许访问 WEB 应用服务器的 HTTP 端口等。

外网：包括省级、地市级和营业网点的网络。

在这种配置下，总部办公网络的安全保证较差，有可能会受到来自分支机构内网的攻击。为此，我们建议通过交换机和路由器的安全配置（包括安全路由设置、网段划分、VLAN 设计等）进行保护。

通过配置防火墙，实现了网络层的访问控制，但是防火墙的访问控制粒度很粗，一般只对 IP 地址、TCP/IP 服务端口进行控制，只能在网络层提供基本的访问控制，不能满足对应用系统和其数据的安全需求。企业网络中应用系统的访问控制需求更复杂，需要采用其他一些安全措施。我们将在后面进行分析。

8.4.6 入侵检测系统设计

我们建议针对企业网络的服务器网段，配置实时的入侵检测系统，以及时发现并阻断各种可能的网络攻击企图。

入侵检测系统有基于主机和基于网络的两种模式的技术和产品。

基于网络的入侵检测系统，通过在计算机网络中的某些点，被动地监听网络上传输的原始流量，对获取的网络数据进行处理，从中获取有用的信息，再与已知攻击特征相匹配，或与正常网络行为原型相比较，来识别攻击事件。

基于主机的产品只能针对某一个服务器的访问行为进行检测，一般是通过检查系统的访问日志进行判别，识别率较高，但实时性较差。此外，基于主机的产品与服务器的操作系统关系密切，一般只支持主流的操作系统（如 Windows NT，Solaris 等）。

为此，我们建议采用基于网络的入侵检测系统，配置如下。

（1）在总部网络的非军事化区，配置一个入侵检测系统的探测头（入侵检测引擎），监控非军事化区内的所有服务器（包括应用服务器、电子邮件服务器等）和主机（如各种系统的管理终端）是否受到攻击，并在有攻击发生时进行报警、阻断和记录等。

（2）在总部网络的安全内网，配置一个入侵检测引擎，监控对安全内网中的所有服务器（主要是数据库服务器）和主机是否受到攻击，并在有攻击发生时进行报警、阻断和记录等。

（3）在总部局域网的非军事化区，配置入侵检测系统的监控中心，对所有入侵检测引擎进行集中、统一的管理和监控。

国外的入侵检测产品以 ISS 公司（安氏公司）的 RealSecure 为代表。ISS 公司是国际最著名的网络安全公司之一，其 SAFESuite 产品是国际上最早推出的网络安全漏洞扫描和实时入侵检测系统，并一直引导着漏洞扫描和入侵检测产品（IDnA）的技术潮流。ISS RealSecure 产品是技术最先进，功能最强大，能够检测最多的攻击行为，并且误报率较低。

入侵检测系统主要是利用根据网络上的各种网络攻击（黑客攻击）的特征数据包生成的攻击模式库，对网络上的各种数据包进行匹配，检查是否与某种网络攻击的特征数据包相符，因此对于网络上各种针对服务器操作系统、网络服务的网络攻击（我们一般称之为“黑客攻击”或“外部攻击”），能够很好地防范；而对于以窃取数据为目的的各种攻击

（其攻击方式主要有用户身份假冒、非授权访问、网络侦听等，我们一般称之为“内部攻击”）并不能很好地防范，必须采用应用层的安全技术进行防范。

8.4.7　网络平台安全子系统小结

在网络平台安全子系统中，我们主要分析了网络的安全拓扑、防火墙、入侵检测系统等安全技术及其安全设备的配置。

网络平台的安全还需要保证网络设备，如路由器、交换机的配置是安全可靠的，另外还可以采用 VLAN 划分技术等保证企业网络平台的安全。

8.5　系统平台安全子系统

在安全体系框架中，系统平台安全子系统涉及到用户认证、访问控制、主机上存储的数据的完整性和保密性、访问的审计、主机及其上的服务的可用性和可靠性等安全服务，一般采用增强操作系统安全、主机安全扫描、主机入侵检测、主机防病毒、文件存储加密、数据库存储加密等措施。

8.5.1　系统平台安全需求分析

系统平台的安全需求主要是保证主机，特别是各个应用服务器和数据库服务器的操作系统、应用服务器及其数据的安全。

Internet 上的各种网络攻击主要集中在系统层，包括对各种操作系统（如 Windows NT/2000、各种 UNIX、Linux 系统等）、网络基本服务（如 FTP、TELNET、HTTP）、应用服务器（如 WEB 服务器、数据库服务器等）等的攻击，利用这些操作系统、网络服务、应用服务器的安全漏洞，取得对服务器的控制权。常见的网络攻击类型包括端口扫描、IPC 攻击、CGI 攻击、数据库口令猜测、强力口令破解等以及针对特定服务的攻击，如 FTP、TELNET、FINGER、MS IIS Web Server 等。这些攻击也可能在企业内网出现。

此外，病毒也可能进入企业内网并传播开来，对各种服务器和桌面机造成破坏，导致系统不可用、文件损坏、数据丢失等严重后果。

因此在企业内网当中，系统平台安全子系统的目标主要是：

（1）保证服务器操作系统和应用服务器的安全，尽量选用比较成熟的操作系统，对于商业操作系统要及时为其打上补丁包，在应用服务器上，不必要的服务坚决关掉。

（2）防范病毒在企业内网内的传播和破坏，及时发现、消灭进入企业内网的病毒。

根据这些安全需求，我们认为系统平台安全子系统的解决方案应该包括：

（1）计算机操作系统的安全配置，主要是系统安全管理员的管理职责；

（2）采用安全漏洞扫描和评估系统，对现有网络中的服务器、主机进行扫描，预先查找出存在的漏洞，以便进行修补；

（3）建立一个完善的防病毒体系。

8.5.2　系统平台安全域的划分

由于系统平台的管理对象主要是部门的服务器和桌面机，因此我们建议每个部门划分

独立的安全域，每个安全域内的安全管理员独立管理本部门局域网内的服务器和主机，独立完成服务器的安全配置，加强现有系统的安全性，建立独立的防病毒体系。

8.5.3 服务器安全配置

我们从 UNIX 和 Windows NT 两方面进行介绍。

1. UNIX 系列操作系统的安全配置

UNIX 系列操作系统包括各种常见的 UNIX 操作系统，如 SUN Solaris、HP UX、IBM AIX 以及各种 Linux 操作系统，如 RedHat、FreeBSD 等操作系统。

当前网络黑客攻击的基本方法是利用操作系统或网络基本服务的各种漏洞，取得一个一般用户的账号，在此基础上进一步取得一个超级管理员的账号，然后在系统中设置各种后门、木马程序，实现对系统的完全控制。

因此，UNIX 系统安全性主要通过以下几种方式实现。

（1）严密保护账号口令

严密保护用户账号和口令，防止外泄是非常必要的，必须采取以下保护措施：

① 账号和口令的持有者应严守秘密，不要轻易将账号和口令交给他人或随意放置，绝对不能泄露系统管理员的账号和口令；

② 口令设置应尽可能复杂一些，并最好能做到经常更换，防止非法用户轻易猜出口令；

③ 在 UNIX 系统中创建用户时，一定要注意用户 UID 的选用。因为如果两个用户具有相同的 UID，他们将互相读写彼此的文件、删除彼此的进程等，这对于 UNIX 系统是很不安全的，必须确保每个用户都具有唯一的 UID。另外，千万不要将根用户或超级用户的 UID（即 UID 为 0）随意用于任何一般用户，因为超级用户具有访问系统中的所有文件，删除系统中的所有进程等功能；

④ 在选用用户的 GID 也应该特别慎重，因为同一组的用户可以互相访问彼此的文件。

（2）适当控制文件许可权和拥有权

文件的使用权限对于 UNIX 系统安全来说是十分重要的，随意地分配文件的使用权限，将可能危害整个系统安全，因此适当地控制文件的许可权和拥有权，也是防范非法侵入的有效方法。

（3）定期检查安全日志和系统状态

为了更有效地防范非法侵入系统，应定期检查安全日志和系统状态。可以选择使用 UNIX 系统提供的对系统的活动进行总览的命令或者阅读 UNIX 系统的安全日志。

（4）慎重使用网络守护服务

UNIX 系统还提供了许多网络守护程序，如 ftp、telnet、shell、login、exec、talk、tftp 等，这些网络守护程序对系统安全影响很大，应注意慎重使用这些网络守护程序，如无实际应用，在信息网络中所有的 UNIX 系统中都禁止这些服务。

（5）及时为系统打上补丁

UNIX 系统中很多的服务，包括一些基本的网络应用，如 HTTP、FTP、SNMP、SENDMAIL 等都存在很多安全漏洞。因此，系统管理员要积极关注有关网站上对这些网络服务的漏洞的报告，有补丁的要及时打上补丁，还没有补丁的要采用相应的防范措施，如暂时停止服务等。操作系统包括各种服务不一定要使用最新的版本，相反，版本稍低一点

的应用一般来说都比较成熟，补丁也比较充分。

2. Windows 系列操作系统的安全配置

包括 Microsoft Windows 系列的操作系统，如 NT/Windows 2000 等系统的一般性安全配置，主要有以下几方面。

（1）严格用户账号管理

① 加强信息网络用户账户的管理，限定用户账户的访问权限，明确规定账户的口令限制和账户的锁定参数。

② 严格限制 Administrator 组和备份组账户的成员资格。

由于 NT 的安全账户管理（SAM）数据库可以由以下用户被复制：Administrator 账户，Administrator 组中的所有成员，备份操作员，服务器操作员，以及所有具有备份特权的人员，而 SAM 数据库的一个备份复制能够被某些工具利用来破解口令，所以必须对那些具有复制 SAM 数据库权限的特殊用户账户资格进行严格筛选，同时加强对这些账户的跟踪，尤其是 Administrator 账户的登录（Logon）失败和注销（Logoff）失败。对 SAM 进行的任何权限改变和对其本身的修改进行审计，并且设置发送一个警告给 Administrator，告知有事件发生。

另外，为了防止特洛伊木马（Trojan Horses）及病毒的入侵，所有具有 Administrator 和备份特权的账户绝对不能浏览 Web。所有的账户只能具有 User 或者 PowerUser 组的权限。

③ 将系统管理员 administrator 账号改名，以防非法用户对系统管理员账号进行口令攻击。如果用的是 NT4.0，可以用 Resource Kit 中提供的工具封锁联机系统管理员账号，这样可封锁由网络而来的非法登录。

④ 对于在信息网络中用于提供公共服务信息的服务器不需要也不应该有除了系统管理用途之外的其他用户账号。因此，应该废止 Guest 账号，移走或限制所有的其他用户账号。

（2）用 NTFS 取代 FAT

信息网络中的各个基于 Windows 系列的服务器要尽量采用 NTFS 而不用 FAT 文件格式，并限制用户对 NTFS 卷上的磁盘、目录或文件的访问权。

NTFS（NT 文件系统）可以对文件和目录使用 ACL（存取控制表），ACL 可以管理共享目录的合理使用，而 FAT（文件分配表）却只能管理共享级的安全。使用 NTFS ACL 的好处在于，如果它授权用户对某分区具有全部存取权限，但共享级权限为“只读”，则最终的有效权限为“只读”。Windows NT 取 NTFS ACL 和共享权限的交集。

（3）认真设置并正确利用审计系统

通过激活 Windows NT 的事件审计系统，可对在 NT 环境中安全性是否已经被攻击或攻破作一很好的监控与分析。通过审计各种操作成功和失败的情况（失败的情况通常比成功的情况少得多），管理员可随时排除安全隐患；另外不常用的操作也值得注意，如安全性策略的改变和再启动往往反映了未经授权的行为。

审计日志本身也需要保护，因为非法用户在进入系统之后通常会抹掉其活动踪迹。首先我们应该定时自动备份日志文件，但是如果这些备份仍然是联机的，则也有可能被非法用户找到。一个比较好的解决方法是将审计事件记录同时制成硬拷贝，或者将其通过 E-mail

发送给系统管理员。

（4）认真利用 NT 域管理及域之间的委托关系

利用 NT 域的管理能力，选择安全策略和操作步骤，把服务器和工作站组成逻辑组，以便于更好地管理信息网络中 NT 服务器和 Windows 工作站。

正确控制信息网络中各 NT 服务器域的委托关系，从而控制网络用户的访问权限，使机关局域网中资源只在一定范围内进行共享。

（5）确保 ERD 更新后对 SAM 数据库的防护

每次紧急修复盘（Emergency Repair Disk－ERD）在更新时，整个 SAM 数据库被复制到%system%/repair/sam。为防止非法入侵，必须确保在每次 ERD 更新后，%system%/repair/sam 对所有人不可读。严格控制对该文件的读权，甚至是不要给 Administrator 访问该文件的权利，如果需要更新该文件，Administrator 暂时改变一下权利，当更新操作完成后，Administrator 立即把权限设置成不可访问。

（6）及时安装最新的补丁包

与任何一个系统一样，Windows 系列操作系统也存在很多安全漏洞，这些漏洞往往是在被发现之后才由 Microsoft 的技术人员制作一些补丁包来加以弥补修正。所以，为了最大程度地减少 Windows NT 中的 BUG 可能给企业网络带来侵害，除了针对这些漏洞对 NT 操作系统作一些策略性的设置外，另一个重要且有效的方法就是及时安装微软所提供的补丁包。

8.5.4 漏洞扫描和评估系统

为了事先发现各个应用服务器的操作系统和应用系统的安全性，可以采用漏洞扫描系统对重要的服务器先进行扫描，以发现系统中可能存在的安全漏洞和安全薄弱环节，先一步采取适当的补救措施（如安装补丁包、升级服务程序、停止不必要的服务、禁止某些用户账号等），达到防范的目的。

漏洞扫描和评估系统可以针对企业网络中的各种网络设备、防火墙设备、应用服务器、数据库服务器和桌面机进行扫描，可以检测出：

（1）被扫描对象的操作系统及其版本，该版本已知的各种安全漏洞，是否有补丁包；

（2）被扫描对象上存在的各种应用服务程序及其版本，该服务的各种已知安全漏洞。

（3）被扫描对象上存在的后门和木马程序。

（4）被扫描对象上的用户列表，并可以检测出其中不安全的用户账号，如某些没有设置口令，或口令很不安全的用户账号。

好的漏洞扫描系统可以用形象的图表表示出在一个网络中的安全薄弱环节，并可以提供非常有用的补救建议。

但是，和入侵检测系统一样，漏洞扫描系统主要是针对因特网上的各种网络攻击，利用攻击模式库，对系统的安全漏洞进行检查，而对于内部攻击的安全隐患并不能很好地检测出来。

此外，漏洞扫描系统在网络当中并不是一个实时启动的系统，只需要定期挂接到网

络中，对当前网段上的重点服务器（如 WEB 服务器、数据库服务器、邮件服务器、DNS 服务器、主域服务器等）以及主要的桌面机进行一次扫描，即可得到当前系统中存在的各种安全漏洞。只要管理员及时采纳了其补救建议，即可在相当一段时间内保证系统的安全（当然还需要管理员及时跟踪最新的安全漏洞和攻击手段，以免成为新发现的安全漏洞的受害者）。

因此我们不建议直接购买漏洞扫描产品，可以采用购买服务的方式，由安全服务提供商对网络内的服务器、主机进行检查。

8.5.5　企业防病毒体系

1. 企业级防病毒体系设计原则

计算机病毒防护是计算机系统安全策略中的重要组成部分，计算机系统的安全运行、数据文件的安全使用是保证企业网络正常运作的重要环节。

伴随计算机应用技术的发展，网络文件传输、电子邮件和国际互联网的日益盛行，病毒的种类和传播媒介都在不断翻新，病毒不仅可以通过软盘传播，更多地通过网络共享文件、电子邮件及 Internet/Intranet 进行扩散。

企业网络中数据库、文件数据交换和电子邮件的大量应用，面临传统病毒和新一代病毒造成的巨大威胁。为此，我们认为必须在企业网络中，规划好防病毒体系。

在设计企业网络防病毒体系时，我们建议遵循下面的原则：

（1）层层设防，逐层把关。根据病毒传播的可能途径，在最恰当的位置配置防病毒软件，扫描、清除病毒，切断病毒的传播来源和途径，把病毒影响限制在最小的范围之内。

（2）分布配置、集中控管。防病毒软件要配置在对清除病毒最能起作用、最有效、最迅速的地方，同时在网络环境下，所有的防病毒软件要能够实现集中的管理，要能够自动分发、自动安装、统一升级，这样一方面可以减轻管理员的工作量，同时又有效地防范病毒在信息网络中的传播，特别是对网络病毒的清除，更需要在全网范围内的统一协调的管理。

2. 企业级防病毒体系设计

网络环境下的防病毒必须层层设防，逐层把关，堵住病毒传播的各种可能途径，包括：

（1）网关防病毒

Internet 是现在病毒传播的一个最主要的路径，访问 Internet 网站可能会感染蠕虫病毒，从 Internet 下载软件和数据可能会同时把病毒、黑客程序都带进来，对外开放的 WEB 服务器也可能在接受来自 Internet 的访问时被感染上病毒。

在企业网络中，不同机构局域网之间的访问，可能会引起病毒在不同机构局域网之间的传播，因此，我们建议在每个局域网与其他局域网之间，配置防病毒网关。

（2）邮件防病毒

邮件附件是当前网络病毒传播的一个重要途径，因此要在邮件服务器上配置邮件防病毒软件，检查所有从邮件服务器发送和接收的邮件，特别是其邮件附件。

在企业网络中，设计两套电子邮件系统：一是加密的专用电子邮件系统，其病毒免疫能力可以得到保证；其二是基于企业网络应用系统的通用电子邮件系统。

我们建议在通用邮件服务器上配置邮件防病毒服务器。针对该邮件服务器的类型，可以选择针对不同邮件服务器的防病毒软件，如 Sendmail、Lotus Notes、Exchange 等。

另一方面，防范邮件病毒传播要加强对用户的安全教育，对于所有来源不明的邮件不要轻易打开，特别是其附带的邮件附件。在打开邮件之前，最好打电话与发件人确认，因为很多邮件病毒是自动从通信录中查找收件人的。发送邮件时，最好不要使用复杂的格式，可以直接使用纯文本格式，这样邮件带病毒传播的机会就很小了。

（3）服务器防病毒

对重要的服务器，特别是 NT 主域服务器，要配置服务器防病毒软件。

我们建议在企业网络中为基于 Windows NT/2000 各个服务器（如域服务器、应用服务器、数据库服务器、邮件服务器、Web 服务器等）都配置服务器防病毒软件。如果邮件服务器是基于 NT 平台的，则不但要配置邮件防病毒服务器软件，还要配置服务器防病毒软件。

（4）主机防病毒

软盘和光盘是病毒传播的另一个主要途径，因此必须针对单机配置主机防病毒软件。

在针对病毒传播的各种途径配置防病毒软件之后，我们在非军事化区内配置防病毒的管理中心。通过该管理中心对整个总部安全域的防病毒系统进行统一的配置和管理，包括防病毒软件包的自动分发和安装、病毒库的自动更新、病毒检测引擎的自动升级等。这样只需要管理员及时关注病毒的发展动向，及时下载最新的病毒库和病毒检测引擎，及时升级防病毒管理中心的防病毒软件和病毒库，就可以把最新的防病毒软件和病毒库部署到整个总部局域网，及时查杀各种病毒。

需要说明的是，现在网络病毒发展更加迅猛，往往能在几个小时之内通过互联网传播到世界各地。而防病毒厂商从发现某种病毒到制伏、提出解决方案、升级病毒库或更新病毒检测引擎往往需要一段时间，而在这段时间内，病毒就可能已经侵入网络并散播开了，甚至造成了破坏。

因此，并不是说配置了企业级防病毒体系，就可以高枕无忧了。以管理员为主的所有用户都要时时关注病毒的发展动向，在第一时间内做好防范措施。

对于非专业用户来说，这个要求比较高，因此我们建议选择能够提供良好安全服务的专业厂商，建立长期的固定合作，以充分保障对病毒和其他安全风险的防范。

8.6 应用平台安全子系统

应用安全子系统涉及到在安全体系框架中提及的各种安全服务，如对应用系统的用户认证、访问控制、数据的完整性和保密性、抗抵赖、审计及应用系统的可用性和可靠性，因此这是最复杂的一个安全子系统，可以采用的安全措施有：使用应用开发平台提供的各种安全服务，在应用系统中开发各种安全服务，使用第三方应用安全平台提供的安全服务等。

8.6.1　安全管理对象和安全域划分

应用平台安全子系统的安全管理对象是在企业网络上运行的各种应用系统，其安全目标主要是防范各种内部攻击。

表 8-1 列出了外部攻击和内部攻击的一些主要区别。

表 8-1　外部攻击和内容攻击的比较

比较项目	外 部 攻 击	内 部 攻 击
攻击目的	篡改 Web 页面，扬自己的名声；使系统不能提供正常的服务；破坏操作系统的系统文件	窃取数据，特别是非授权访问，一般需要避免破坏系统的正常运行
攻击对象	一般是 Web 服务器和 Web 页面，也可针对应用服务器的操作系统	一般是应用系统和应用系统中的数据
攻击来源	来自 Internet 的用户，遍及国内外，无法确定其来源	企业网络的内部用户，在物理位置和网络结构上可以确定
攻击方式	利用操作系统或应用系统已公开的漏洞进行攻击	利用应用系统中可能存在的后门、隐通道、陷阱等进行攻击
攻击手段	CGI攻击 拒绝服务攻击 RPC攻击 IPC攻击 ……	通过技术手段（网络侦听）和非技术手段（社交、偷窥等）窃取合法用户身份； 利用合法的用户身份登录应用系统； 查阅在自己权限之外的信息； 网络侦听窃听重要的数据传输
防范措施	防火墙、漏洞扫描、入侵检测、防病毒	应用系统的代码安全性分析； 应用安全平台

1．长期规划

根据企业网络的整体规划，需要把总部、省级分支机构、地市级分支机构以及营业网点的局域网进行连通，因此，最终每个机构都会有自己的各种应用系统（包括办公系统和业务系统）在企业网络上运行。

在这种情况下，不同部门之间，以及在同一部门的不同层次，对应用系统的管理基本都是独立管理的，每个单位都需要能够管理自己的应用系统，而不能够由一个机构集中管理。否则很容易造成管理上的混乱。

在这种分布式应用环境下，应用系统和数据分布在各自的局域网中，各单位可以把一些数据放到公共服务器上（非军事化区内的 Web 应用服务器）供其他单位的用户查询，但是外单位的用户的访问必须得到本单位的授权。

同样，在一个单位内部，对这些应用服务器的访问也必须得到严格的控制，包括严格的身份认证、细粒度的访问控制、高强度的加密传输和安全的审计记录。

为此，我们建议企业信息网络中，根据不同的部门划分成多个独立的安全域：

（1）财务部门、行政部门、营销部门、人事部门分别是一个安全域；

（2）各省级分支机构分别是一个安全域；

（3）各地市级分支机构、营业网点分别是一个安全域。

2．安全域划分和其扩展性

企业网络第一步主要是在总部建立一个通用办公平台，其应用服务器和数据库服务器都集中在总部。

很明显，对这个应用系统的管理权限集中在总部，可以由总部的安全管理员控制哪些用户能够访问该应用系统，能够访问什么样的信息和资源。

8.6.2 应用平台安全子系统设计思路

为了有针对性地设计应用平台安全子系统，我们必须从分析应用系统的安全机制入手，对其安全需求作出准确的判断，针对应用系统中安全机制比较薄弱的环节，采取相应的安全措施，以达到在企业网络中运行应用系统、传输机密数据的目的。

8.6.3 应用系统安全机制分析

应用系统的主要安全机制包括以下几点。

（1）用户管理

由应用系统在数据库中维护所有能够进入该应用系统的用户目录，这里的用户是一些具体的人（如张三、李四）或角色（如经理、总监等）。

（2）资源目录管理

由应用系统在数据库中维护应用系统的资源对象，传统的资源对象概念包括应用系统的各个子模块和各个更小的模块，扩展的资源对象概念包括对某类信息的一种处理操作。扩展的资源对象概念一般应用于Web应用模式，每一个CGI程序就是一个资源对象。应用系统中所有资源对象的集合称之为资源目录。

（3）授权管理

由应用系统预先设定用户对资源对象的访问权限，如经理可以执行领导查询系统，张三可以执行公文撰写操作等。

（4）用户身份认证

用户访问应用系统时，要求用户提供一个身份，应用系统根据用户表检查该身份是否合法。当用户自称的身份得到认可之后，用户可以进入应用系统访问资源。

（5）访问控制

当用户通过身份认证之后，根据用户身份及其访问的资源对象，查找权限库，授予用户相应的权限，如允许张三录入公文等。

（6）此外，在应用系统中还有传输加密、审计日志等需求。

上述应用系统的安全机制及其工作过程如图8-2所示。

（1）应用系统管理员通过应用系统管理模块维护好用户表、ACL表（各种用户的各种权限组合）、资源目录表、访问控制表（用户对资源的访问权限）；

（2）用户提交访问请求，并提交一个身份（如用户名或角色）；

（3）应用系统通过身份认证模块认证用户提交的身份；

（4）应用系统通过访问授权模块取得用户对所访问资源的访问权限；

（5）应用系统根据权限决定用户的访问请求是否能执行，完成数据处理；

（6）应用系统把请求的处理结果返回给用户；

（7）根据需要，在上述应用过程中，需要采用传输加密和审计等功能。

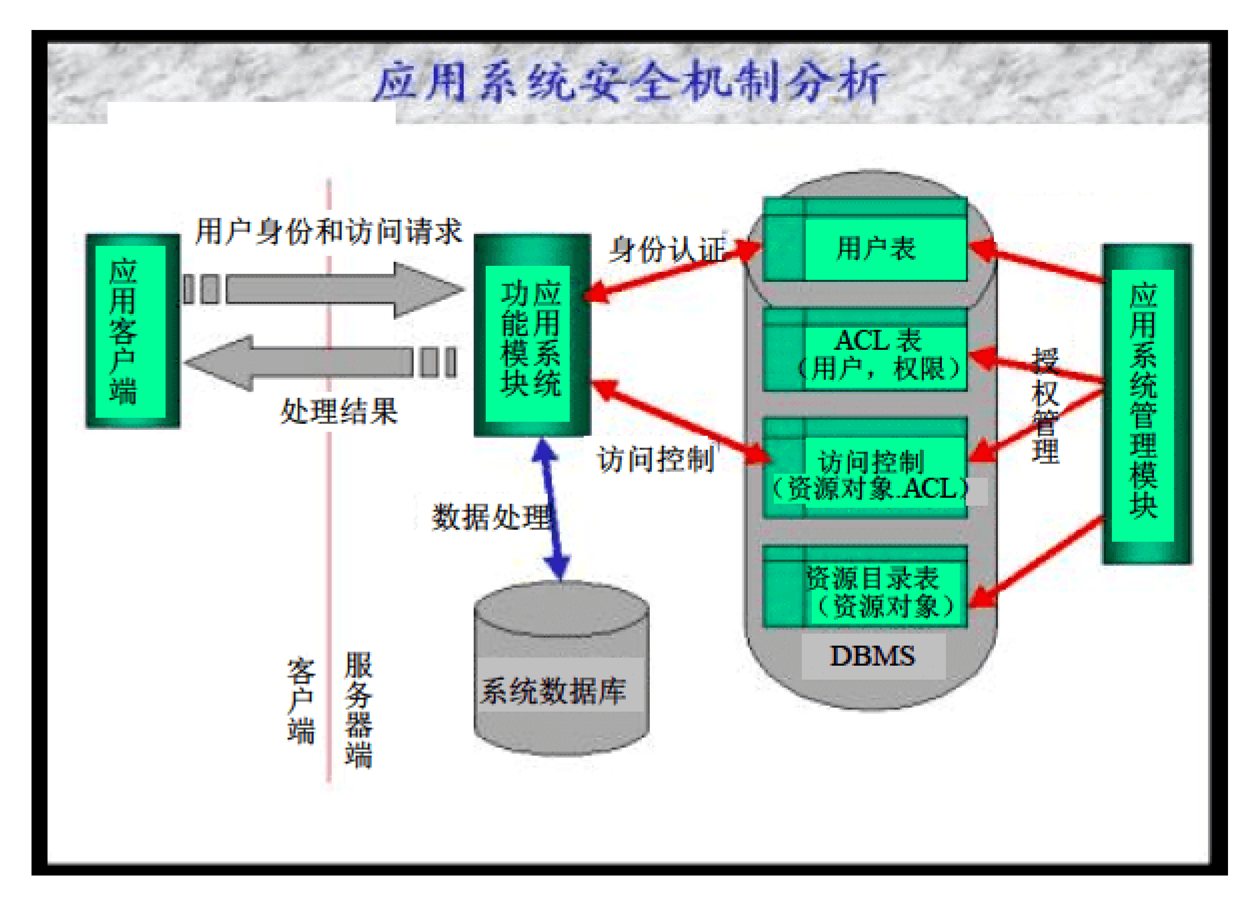


图 8-2　应用系统安全机制

8.6.4　应用系统安全风险分析

应用系统存在的安全风险主要有以下几个方面。

（1）用户身份假冒

非法用户利用合法用户的用户身份（用户名、口令），访问系统资源。其风险来源主要有两点：一是应用系统的身份认证机制比较薄弱，如把用户信息（用户名、口令）在网上明文传输，造成用户信息泄露；二是用户自身安全意识不强，如使用简单的口令，或把口令记在计算机旁边。

（2）非授权访问

非法用户或者合法用户访问在其权限之外的系统资源。其风险来源于两点：一是应用系统没有正确设置访问权限，使合法用户通过正常手段就可以访问到不在权限范围之内的资源；二是应用系统中存在一些后门、隐通道、陷阱等，使非法用户（特别是系统开发人员）可以通过非法的途径进入应用系统。

（3）数据窃取

攻击者利用网络窃听工具窃取经由网络传输的数据包，通过分析获得重要的信息。

（4）数据篡改

攻击者篡改网络上传输的数据包，使信息的接收方接收到不正确的信息。

（5）数据重放攻击

攻击者抓获网络上传输的数据包，再发送到目的地。

（6）抵赖

信息发送方或接收方抵赖曾经发送过或接收到了信息。

在企业网络中，应用系统的安全风险主要是用户身份假冒和非授权访问。同时，也要求数据在网络上传输时必须有高强度的加密处理。

这些安全风险必须采取“安全管理为主，安全技术为辅”的措施解决。

在安全管理方面，主要是制定各种安全管理制度，加强对用户的安全意识和安全技术的培训，使每一个用户都切实意识到安全问题的重要性，遵循安全管理制度，结合相关的安全措施，采取各种安全手段，如选用各种复杂的口令、严密保管自己的用户名和口令、启动有关的安全软件、离开工位时马上退出应用系统，清除自己的登录信息等。

在安全技术方面，主要针对上述安全薄弱环节，采取相应的安全措施，如加强身份认证的安全机制、严格应用系统的授权管理、采取高强度的加密措施等。

8.6.5 应用安全平台需求分析

针对上面提到的应用系统的安全风险，传统的解决方案主要是依赖应用平台，如数据库、Notes、Web Server等自身的安全机制，在应用系统开发时，由开发人员设计安全体系，建立用户、给用户授权。其主要优点是与系统结合紧密，但是存在其他一些问题：

（1）开发工作量大

据统计，传统的应用系统开发中，安全体系的设计和开发约占开发量的三分之一。当应用系统需要在互联网上运行时，随着安全需求的增加，其开发量占的比重会更大。

（2）安全强度参差不齐

根据应用平台的安全机制的完善程度，设计、开发人员对安全体系的理解程度以及投入的工作量，不同的应用系统的安全强度会相去甚远。

（3）安全没有保障

目前很多应用系统设计、开发人员的第一概念是系统能够运行，而不是系统能够安全运行，因此在系统设计、开发时对安全考虑很少，甚至为了简单或赶进度而有意削弱安全机制。有些应用开发人员甚至可能会在应用系统中设置一些很难察觉的后门、隐通道和陷阱等，直接威胁到应用系统中数据的安全。主要可能有下面的安全隐患。

① 身份认证机制强度不够。身份认证是应用安全的基础，只有确保用户只能使用自己的身份进入系统，才能保证整个应用系统的授权控制可以正确实施。在传统的应用系统开发中，包括各种主流的数据库平台，使用的身份认证机制都很简单，如使用明文的用户名/口令机制等。因此很容易被攻击者通过侦听或强力攻击等措施取得。

② 访问控制在程序中实现，维护比较复杂，当需求发生变化时，可能会涉及到对应用程序源代码的修改；如果采用 Web 服务器的访问控制机制，只能控制到文件和目录一级，不能完全满足需求，特别是 B/W/D 应用的访问控制需求。

③ 没有采用数据传输加密技术，敏感信息在网络上明文传输，极易被窃听。有些采用了简单的加密技术，很容易被攻破。

④ 不能保证系统没有后门或隐通道。数据库服务器和应用服务器都会有存在后门和隐通道的危险，在管理员不知不觉的情况下，攻击者就可以通过这些后门和隐通道获取敏感数据。

（4）维护复杂

每个应用系统的安全机制各不相同，导致很多重复性工作（如建立用户账号等）；系统管理员必须熟悉每个应用系统独特的安全机制，工作量成倍增加。当某个应用系统的安全策略发生变化时，往往需要修改程序的源代码。

（5）用户使用不方便

用户使用不同的应用系统时，都必须做相应的身份认证。当用户需要访问多个应用系统时，会有很多用户名、口令需要记忆，可能会需要有专门的密码本，或使用相同的简单口令，这实际上将降低系统的安全性。

为此，我们采用经过认证的第三方应用安全平台，为企业网络的应用系统提供安全服

务平台和安全管理平台。对这个第三方应用安全平台，有以下要求。

① 应用安全平台产品必须能够提供全面的、强壮的安全服务，包括严格的用户身份认证、细粒度的访问控制、高强度的数据传输保密性和完整性、详细的审计记录等。应用安全平台是应用系统的安全入口，因此，其自身的安全性将直接影响到整个应用系统的安全。

② 应用安全平台产品必须能够为企业综合信息网现有的，以及以后将要上的各种Web应用和传统的C/S结构应用提供一个统一的安全平台。

③ 这个应用安全平台同时也是一个安全管理平台：这个应用安全管理平台必须提供全局的用户、资源和授权策略的管理功能。

各种应用系统的分散安全管理是造成应用系统安全隐患的主要原因，通过集中管理，管理员通过应用安全平台的管理控制台就可以看见各种安全因素，如应用系统的用户、管理的资源以及赋予用户对资源的访问权限，因此一方面可以减轻系统安全管理员的工作量，更主要的是可以避免各种安全隐患。

④ 应用安全平台和应用安全管理平台要有机地结合起来，形成一个既能为应用系统提供高强度、可靠的安全服务，又能为应用系统维护人员提供简便、快捷、安全、可靠的系统维护管理的应用安全平台。

8.7　网络安全规划案例

下面是一个网络安全规划案例，其中 A 公司是一家虚拟公司。由于人们日益关注计算机网络的安全性，公司决定评审安全措施，并制定改善这些措施的计划。通读该计划可以提供一个很好的思路和步骤，帮助制定有效的网络安全规划。

8.7.1　背景简介

网络安全规划的制定工作由 IT 经理（或者网络管理员）制定，最后得到老板（或者总经理）的认可，公司其他人员可以提供建议和意见。

1. 关于 A 公司

公司拥有 20 名员工，专门提供旅游服务。员工包括设计师、旅行代理和营销人员以及为他们提供支持的行政团队。企业高层管理人员包括：合伙创始人总经理和运营总监，以及财务总监。

2. 规划目标

此安全规划是公司第一次做网络安全规划。它将广泛关注公司所面临的安全风险，并及时采取措施以降低我们的风险。在过去的半年中曾发生过一次大规模的病毒攻击事件，希望通过合理的安全规划，避免那样的灾难再次发生！而且，希望通过更广泛的关注，能够预防目前尚不了解的安全威胁。

不管是时间、人力，还是财力都很有限。继续成功开拓业务是公司的首要任务。项目团队在决定怎样做时仔细权衡了这些限制条件，并努力在实用性、成本、舒适程度和安全措施之间实现平衡。最后一致认为，无所作为决非上策。

安全规划已经通过评审，决定实施该计划，而且取得公司领导的重视，把此计划作为公司优先级较高的一项任务来进行。

3．规划文档传播

本安全规划文档中包含重要的安全信息，因而它属于机密文档。不能随意放置或复印。 也不能通过电子邮件发送或将其存储在服务器上，只使用书面副本。授权以下人员查阅本文档：

总经理

运营总监

财务总监

经理助理

公司律师

安全顾问

4．项目团队

项目团队包括：

项目经理（运营总监）

财务总监

经理助理

安全顾问对我们的员工提出意见，并参与部分意见的实施。

此外，我们还与销售、营销和设计人员进行协商，获取他们对自己希望的情况以及计划可能会对他们造成的影响提出反馈意见。

8.7.2 评估结果

经过我们的评估，得出了以下结果。

1．技术和知识

我们的技术安全顾问熟悉我们的系统和公司安全，他将为我们提供专家级指导。但是，我们需要尽可能多地做工作，以让我们自己尽可能多地掌握这方面的知识。这样做还有助于我们节省资金。

项目团队的每位成员均阅读了 Microsoft 和 Internet 工程任务小组 (IETF) 提供的安全计划指南，以便做好准备。公司员工都具备相当丰富的技术知识，但是绝大多数员工都将计算机看作完成工作的工具，而对计算机的工作原理知之甚少。

2．我们的网络和系统

下面是我们的技术设备清单。

台式机：22 台（每位员工一台，另外两台旧计算机用作打印服务器）；

便携式计算机：6 台（每位总监一台，一台供财务总监使用，另有三台供销售团队使用）；

打印机：2 台（一台高端绘图仪和一台用于常规用途的打印传真多功能机）；

服务器：1 台（一台运行 Windows Small Business Server 2003 并且管理 Internet 连接、电子邮件以及我们的客户数据库的计算机）；

Internet 连接：1.5 Mbps 电缆调制解调器连接。服务器和几台计算机通过 100 Mbps Cat5 以太网电缆连接。其他计算机通过具有访问端口的 802.11g 无线网络连接。

除两台打印机服务器和两台行政用计算机运行 Windows 98 外，其他所有计算机均运行 Windows XP Professional。

3. 安全

我们运行了 Microsoft Baseline Security Analyzer。通过执行这些措施，结果如下。

（1）病毒防护：6 台计算机上没有病毒防护；4 台计算机上没有最新的病毒防护；普遍地，大多数用户都能发觉病毒，但是不太清楚如何能够防止病毒。

（2）垃圾邮件筛选软件：许多用户开始抱怨垃圾邮件，但是尚未采取防护措施。

（3）防火墙：我们原以为 ISP 的路由器中包含防火墙，但事实上没有；因此，我们没有防火墙。

（4）更新：所有 Windows XP Professional 系统均为最新，因为该系统可以自动检查和下载更新。 但是，几台计算机上安装的 Microsoft Office 需要更新，并且安装 Windows 98 的计算机根本就没有更新。

（5）密码：随机抽样调查发现，大多数人根本不使用密码，或者将密码写在便笺上并贴在计算机旁边。 特别是，没有一台便携式计算机具有密码保护。

（6）物理安全：窗锁、门和报警器状况良好。 但是，所有计算机的机箱上均未标明序列号，并且我们没有序列号记录。 我们还注意到，所有人（包括 Tracy 和两位总监）都在使用同一打印机，这意味着存在偶然将机密文档遗忘在打印机旁的风险。

（7）便携式计算机：所有便携式计算机均装在印有醒目制造商徽标的便携包中，并且没有安全锁。

（8）无线网络：我们只是建立了网络并使其能够运行，因此没有人改动过任何设置。但是，这证明我们的无线网络对可以查找无线网络并且自由使用 Internet 连接的外部人员是开放的。

（9）Web 浏览：每个人都认为快速 Internet 访问益处多多，但是他们一直都在使用，而没有对风险问题考虑太多。 通过内容筛选审核，我们发现有 20% 的 Web 浏览与工作无关。 我们并没有关于 Web 浏览的规定，并且没有人采取任何安全措施。

（10）备份：我们每周都将服务器上的数据备份到数字音频磁带 (DAT) 驱动器上，但是没有测试是否能够还原数据；除非有人记得将本地文件复制到服务器上，否则将不会备份这些文件，这实在不能令人满意。 服务器包含有我们的主要客户数据库，因此经过认真测试的备份和在非现场位置保存一个备份副本都同样必不可少。

4. 优先级

根据我们的评估，安全优先级如下。

（1）阻止入侵者

- 安装防火墙
- 安装和更新病毒防护
- 增强无线网络
- 使用运行 Windows XP Professional (SP2) 的计算机更换 4 台运行 Windows 98 的计算机
- 确保将所有计算机都配置为自动更新
- 对用户进行培训并说明相关策略

（2）预防盗窃

- 帮助保护便携式计算机

- 盘点和标记资产
- 将服务器搬到安全且可上锁的房间
- 以物理方式保护台式机和便携式计算机

（3）预防灾难

- 制定更好的非现场存储备份方案
- 确保备份用户的本地数据
- 非现场存储重要的书面文档副本
- 通过执行还原操作来定期测试备份

（4）内部安全性和机密性

- 制定强密码策略
- 保证财务部、人力资源部和总监所使用打印机的安全
- 检查档案柜和机密文档的安全

8.7.3 安全计划

进行评估后，我们制定出以下安全计划。

1．行动事项

（1）选择、购买和安装硬件防火墙（或让 ISP 或技术顾问提供一个）。

（2）在服务器和所有台式机上启用 Windows 防火墙。

（3）确保在所有计算机上安装防病毒软件，并且设置为自动更新病毒定义。

（4）将运行 Office Outlook 2003 的计算机配置为使用垃圾邮件筛选功能。 选择、购买并在邮件服务器上安装垃圾邮件筛选软件（如果必要）。

（5）在无线网络上，禁用服务设置标识符 (SSID) 广播，选择和配置有意义的 SSID，启用 WPA 加密，启用 MAC 筛选，并将访问点配置为只允许来自办公室中台式机和便携式计算机的流量。

（6）使用运行 Windows XP Professional (SP2) 的计算机更换四台运行 Windows 98 的计算机。

（7）查看所有计算机以确保均已完全更新，并且将它们设置为自动刷新这些更新。

（8）购买新的且无明显特征的便携式计算机包和锁。

（9）确保标记所有台式机、便携式计算机和它们的组件。

（10）记录所有序列号。

（11）为台式机购买和安装办公桌安全锁。

（12）将服务器放在一间大小合适且可以上锁的房间中。

（13）检查备份和还原过程。在备份之前，确保定期在服务器上存储用户数据或复制用户数据；实施每日备份；确保每周将完全备份转移至非现场位置一次；确保备份受到密码保护，并且进行了加密。 检查书面文档，并且复印在安全的非现场位置存储的重要文档。

（14）将 Windows Small Business Server 2003 和各台计算机配置为强制使用非常强的密码。与用户进行讨论，确定可以接受的方便性和安全性之间的平衡。

（15）将工作站配置为如果工作站处于空闲状态五分钟以上，注销用户，并且再次登录时需要密码。

（16）为财务部、人力资源部和两位总监购买价格便宜的打印机，以便他们可以安全地打印机密文档。

2．响应计划

如果出现违反安全问题，我们将联系安全顾问。 他的公司在办公期间使用一个 1 小时响应策略，在所有其他时间使用一个 4 小时响应策略来解决各种严重事件，例如感染病毒。此外，财务总监定期监控服务器和防火墙，确保不会出现违反安全的情况。

3．持续维护和遵守规程

财务总监负责日常安全，运营总监全面负责。 财务总监将继续钻研该主题，订阅 Microsoft 和防病毒软件提供商的安全公告，并且定期与安全顾问联系，以监督是否符合新策略。

每个月，财务总监将确保更新 Windows 和我们的防病毒软件，以及备份和还原过程正常运行。他也将负责确保正确配置和更新新的计算机设备。

经理助理负责确保对新加入公司的员工就公司的安全策略和过程进行全面培训。

将在 6 个月后全面正式地检查此计划。

8.7.4 资源和预算

1．外部资源

（1）公司律师审阅我们重新编写的员工策略

（2）安全顾问在制定此计划期间提供建议

（3）安全顾问帮助实施

2．内部资源

尽管我们不会直接向自己的员工支付报酬，但是为了明确资源的分配以及这项工作可占用的时间，我们已经授权使用上述的内部员工。

3．资产

除了有形财产外，我们的主要资产包括：

（1）产品设计和营销宣传材料

（2）供应商合同记录

（3）电子邮件数据库和过去电子邮件消息的存档

（4）销售订单和客户数据库

（5）用于在线预订和在线预约的业务系列 (LOB) 软件

（6）存放在不同档案柜中的书面法律记录

所有这些资产都被视为机密，只有在必要时才能使用。此外，它们需要受到保护，并且尽可能安全地进行备份。

4．风险

我们相信风险主要分为 4 类。

（1）入侵者。入侵者包括病毒、蠕虫、对我们计算机资源或 Internet 连接的攻击和恶意使用。这些风险是任何使用连接到 Internet 的计算机的用户都要面临的风险。高风险，高优先级。

（2）外部威胁（竞争对手、心怀不满的前员工、非法谋利者和盗窃者）。他们可能使

用与黑客相同的工具，但却是有意攻击我们；他们也有可能引诱员工提供机密信息，或甚至使用盗取的资料来勒索或诋毁我们。我们需要保护资产的物理安全和电子安全。高风险，高优先级。

（3）内部威胁。无论是意外的还是有意的，员工都有可能误用他们的权限来泄露机密信息。低风险，低优先级。

（4）事故和灾难。火灾、洪水、意外删除、硬件故障和计算机崩溃。低风险，中等优先级。

5．策略变化

经理助理将更新员工手册，以包括关于以下方面的新策略：

（1）电子邮件和 Internet 的可接受用途；

（2）使用密码；

（3）哪些人员可以将公司财产带出办公室。第一份草稿完成后，公司总监和律师会在实施之前进行审阅。

6．用户培训

由于这些变化，我们希望最多提供两个小时的时间，按小组形式进行用户培训。 培训内容包括：

（1）安全的重要性；

（2）密码；

（3）便携式计算机安全；

（4）病毒防护；

（5）安全的 Internet 浏览；

（6）从服务器更新软件和操作系统；

（7）介绍新的员工策略；

（8）确保员工明白不遵守策略的后果；

（9）评估员工对新策略的了解程度；

（10）定期检查新策略的实施情况。

7．项目时间表和责任

（1）前三项首要任务，即防火墙、病毒防护和增强无线网络，将需要我们的安全顾问特别注意。

（2）其余的任务将由我们自己的员工按照优先顺序完成。我们预计前三项首要任务将在一个周内完成，其余的任务将在 30 天内完成。

（3）财务总监负责购买和实施技术革新。经理助理负责所有的策略和培训要求。运营总监将对项目进行指导，并负责出现的任何其他任务。

8.8 安全服务

前面从技术层面介绍了企业网络应该采取的安全措施，主要从划分安全网络拓扑结构、设置防火墙网关、建设企业级防病毒体系、正确配置操作系统和建立应用安全平台等方面

保证信息网络的安全。

但是，这些措施仅仅是信息网络安全的基本保证，更重要的是要正确应用好这些安全技术，采取相关的辅助措施，充分发挥其效益。信息网络的安全是一个动态发展的系统工程和社会工程，需要长期、持久的巨大的财力、物力、人力的投入，需要从组织、管理等方面也采取强有力的措施，才能确保信息网络在 Internet 的大洋中永远坚固、安全、可靠。

1．网络安全是动态发展的问题

从历史发展来看，安全是一个随着信息网络发展而发展的现实问题。DOS 时代的安全基本是主机的物理安全问题，局域网的安全则扩展到了整个企业范围，而 Internet 时代的信息网络安全面对的则是来自全世界的网络探险者、黑客、商业竞争对手，甚至是非常亲密的合作伙伴的窥探、侦测、窃听、欺骗等各种各类的攻击。

从现状来看，Internet 网络安全问题也是日新月异。据有关统计数据显示，在 2001 年 1 月份，全球发生了大约 8800 万起有入侵企图的黑客事件，比 2000 年 12 月份增长了 58%；攻击源国家增长了 13%，从原来的 134 个国家增长为 152 个国家。国防科技大学计算机学院所作的研究课题表明，目前我国 95%与因特网相联的网络管理中心都遭到过境内外黑客的攻击或侵入，其中银行、金融和证券机构是黑客攻击的重点，而如此大面积，且涉及到各行各业的情况实属罕见。以网络病毒为例，全球每天都有几十个新病毒产生，最近，“FunLove”、“Happy Time”、“红色代码”、“蓝色代码”、“SirCam”、“Nimda”等病毒更是个个来势汹汹，防病毒厂商的病毒库几乎每隔几天就得升级，而 Microsoft Windows 系列操作系统则是补丁包刚宣布又出来了新的漏洞。

从发展趋势来看，信息网络的安全日益显示出了其重要性。不同国家、地区之间的政治、军事、文化等冲突也动辄引发一轮又一轮的网络攻击战争，如中美、中日、大陆和台湾之间的多次冲突都曾爆发了大规模的有组织的网络攻击。在这些“战争”中，没有任何国家、地区成为赢家，而最大的受害者莫过于无辜的企业，因为网络遭受攻击给企业带来了很大的经济损失和非常恶劣的社会影响。这些有组织、有目的的网络攻击行为一方面提醒了网络建设者要始终把安全问题放在首位，另一方面也将大大促进网络攻击技术的发展。

2．信息网络的安全实施是一个系统工程

对一个信息网络而言，安全问题涉及身份认证、访问控制、数据保密性、数据完整性、抗抵赖、审计、可用性和可靠性等多种基本的安全服务，涉及 ISO/OSI 所有的七个协议层次（物理层、链路层、网络层、传输层、会话层、表示层和应用层），覆盖了信息网络中物理环境、通信平台、网络平台、主机平台和应用平台等几个系统单元。因此，这是一个立体的、多方位、多层次的系统问题，在规划、设计、实施信息网络的安全系统时也必须用系统工程的方法论来考虑。

很多人眼中的网络安全就是防火墙，这是非常不全面的。因为防火墙仅仅是在网络平台一个系统单元的安全技术，仅解决了网络层的部分安全需求，提供的安全服务只有网络层的节点认证、访问控制等，不能解决整个信息系统所有的安全需求。比如说，一般的公开 Web 服务器都会采用防火墙来保护，可以利用防火墙限制“所有用户都只能访问 Web 服务器的 HTTP 服务（TCP 服务端口是 80）”。在这种情况下，从防火墙外部到 Web 服务器的 HTTP 服务的通道是畅通的，如果 Web 服务器的 HTTP 服务存在安全漏洞，攻击者依然可以利用“被允许的”服务通道对 Web 服务器进行攻击。在黑客攻击中有很大部分是

CGI 攻击，其原理即如此。

在信息网络中，需要对外开放的服务相当多，如 HTTP、EMAIL、DNS、FTP、TELNET 等，以及与数据库应用相关的各种服务，这些服务都存在很多安全问题，需要在配置时综合应用各种安全技术加以防范。

因此，我们在规划、设计、维护、管理信息网络的安全系统时，必须从分析信息网络的安全风险出发，考虑不同系统单元、不同协议层次所存在的安全风险，所需要的安全服务，采用相应的安全技术，使不同的安全技术、安全产品互相补充、互相完善，保证信息网络的安全。

3．信息网络的安全是一个社会工程

在网络安全业界，有一个广为传播的说法："三分技术，七分管理"。安全技术和安全产品仅仅是为信息网络实施安全管理提供了技术层面的手段，而这些技术和产品能否起到其应有的作用，更大程度取决于对这些安全技术的应用，对安全产品的配置，以及在信息网络应用环境下硬件设备、软件系统和用户等各种综合因素的作用。

在信息网络中，用户接口是至关重要的。在采取了各种复杂的安全技术之后，如果系统的最终用户没有足够的安全意识和安全常识，不能正确应用各项安全措施，那么其后果要么是安全系统不能工作，影响信息网络的正常运转，要么是安全系统演出空城计，不能起实际的作用（如在一个安全系统中使用简单的用户密码）。

因此，在安全系统建设工程中，必须充分重视用户的安全，加强对用户安全意识的培训，加强安全常识的教育，加强安全系统的使用培训。

综上，实施信息网络安全系统需要巨大的、持久的投入，同时，这也是一项非常专业、系统的工程，仅仅依靠用户自身的技术力量很难顺利完成。我们建议用户在建设自己的信息网络时，选择一家或几家专业的安全厂商作为长期的合作伙伴，为用户提供周到的安全服务，保证信息网络的安全、可靠、正常的运行。

安全服务的内容包括以下几方面。

安全咨询：最新发现的各种安全风险，如系统漏洞、攻击手段、新的病毒；安全技术的最新发展，新的安全技术，新的攻击防御和检测手段；安全技术的发展趋势；信息网络安全系统建设的方法和步骤等。

安全评估：由资深安全工程师针对用户的信息网络，分析其安全需求和现有网络中的薄弱安全环节。分静态评估和动态评估两类，评估方法有所不同。

静态评估：根据用户提供的网络拓扑结构、应用模式和管理现状，从理论上分析用户信息网络中可能存在的安全隐患、网络的安全薄弱环节，包括网络拓扑结构是否能够满足安全需要、重要服务器和网段是否得到足够的安全保护、用户信息系统中应用系统的应用模式是否足够安全等。静态评估方法可以对信息网络中当前的安全隐患作出比较科学的分析，也可以较好地解决信息网络发展的一些安全问题，但是也可能会出现一些偏差，如过高或过低地估计在某方面的安全问题。

动态评估：在用户书面授权和现场监督下，采用专业的网络安全扫描和评估工具，对用户的信息网络中的各种网络设备、操作系统、网络及应用服务进行扫描和分析，并全面分析信息网络中各种网络设备、操作系统、应用系统和安全系统的日志，提出针对整个信息网络的安全风险评估报告及安全建议报告。

安全策略制定：根据用户信息网络的安全需求，制定统一的安全策略。

安全策略定义：安全策略是制定安全制度、采用某种安全技术、购买相应安全产品等各种行为的依据和指导准则。它包括了一系列的法规、标准和惯例，决定了一个组织怎样管理、保护和分发信息网络内部的敏感信息，反映出在用户访问信息网络资源时受到什么样的控制。

影响安全策略制定的因素：包括环境和风险两方面的因素，其中环境又包括网络拓扑结构、系统和网络设备、应用程序、用户等，风险则包括受到攻击的可能性和受到攻击之后的损害程度。制定安全策略时要充分分析各方面的环境和风险因素。此外，还要考虑企业的财力、技术实力等方面的因素。在整个信息网络中，要制定、采取一套统一、完整的安全策略。对信息网络而言，需要采取什么样的安全措施，在什么时候、什么地方使用什么样的安全技术，都需要由一个统一的安全策略作为指导。在信息网络的不同平台、不同部分，都需要在一个统一的安全策略指导下，采取相应的安全措施。安全策略应由信息网络的最高管理层制定，并要求信息网络的所有用户遵照执行。

安全系统规划：利用科学的方法论和安全漏洞扫描、分析工具，分析信息网络的网络、应用、管理的现状和安全风险，全面、细致地分析信息网络的安全需求，采取各种相关的安全技术，提出针对信息网络的全面的、科学的安全体系规划和完整、可行的整体安全解决方案。安全系统规划的服务内容包括安全策略制定和部分安全评估的内容，需要在安全策略的指导下，根据安全评估的结果，为企业提供全面的整体安全系统规划。

安全系统集成：根据安全系统规划和统一的安全策略，根据信息网络的特点，把不同安全厂商的不同安全技术和产品进行集成。

安全系统维护：国内很多用户在购买安全产品之后，由于没有足够的重视，或因为技术力量较差而不能正确运用，安全产品往往没有配置任何的安全规则，沦落为一种摆设。在这种情况下，信息网络的安全产品“有不如无”：既不能为信息网络提供基本的安全防护，又影响信息网络的性能。

事实上，信息网络安全产品的正确配置比产品自身要更为重要。一个功能相对较简单、单一的产品，如果进行完善的配置，充分发挥出其安全功能，其发挥的作用将远远大于一个功能很复杂然而配置出现失误的庞大的产品。（当然，在选择安全产品时，也必须考虑安全产品自身的安全性。）

另外，在整个信息网络中，每一个安全设备在配置时都必须考虑其在整个安全体系中的位置和效果。安全体系中不同的安全产品是互相作用、互相补充的，任何一个安全设备的管理员都必须对整个安全体系有所了解。

此外，安全产品的配置必须根据安全需求和安全风险的变化及时进行更新。网络安全是动态发展的，安全管理员还必须及时掌握网络安全的发展趋势，了解最新的安全风险，根据需要修改安全系统的配置，随时保证信息网络的安全。“从一而终”的配置是非常不安全的。

安全系统的维护包括自有安全产品的维护，也包括非自有安全产品的维护；包括由自己实施的安全项目的维护，也包括不是自己实施的安全项目的维护。

安全培训：分用户级、应用开发者级和管理员级培训三类。

用户级培训：信息网络安全系统是一项社会工程，信息网络的最终用户对安全的认识

直接影响到信息网络的安全。用户级培训是对最终用户的安全意识、安全技术的培训，使信息网络的每一个用户都能够正确利用现有安全技术，保护自己，保护信息网络。

应用开发者级培训：指导应用系统的设计人员、开发人员树立全面的安全意识、正确利用应用平台的安全功能和应用安全平台的安全功能，开发出安全的应用系统。

管理员级培训：对系统管理员的安全技术培训、安全专业知识的培训，培训对象包括网络管理员、服务器管理员、应用系统管理员、安全系统管理员等。

应急安全服务：在紧急情况下，由安全工程师为用户提供事件紧急响应和安全修复服务。将为遭受入侵破坏的用户提供一流安全专家紧急出动服务和安全专家现场服务，并配合计算机安全监察部门对安全事件进行现场保护、审计分析、调查取证和系统修复工作。提供 24×7 的全时安全服务，在发生紧急事件的情况下，安全工程师将在指定时间内到达，采取紧急补救措施，并对事件进行细致的调查取证，最后进行全面的安全恢复。

习题

1．简述网络和应用现状分析包括哪些内容。
2．简述网络安全需求分析包括哪些内容。
3．简述网络安全体系设计准则。
4．简述网络安全体系框架包括哪些内容。
5．简述网络安全包括几个子系统，每个系统的具体内容包括哪些。

第 9 章　网络安全实施

教学提示

经过前面几章的学习，读者对网络安全的常用技术、计算机安全、局域网安全、广域网安全以及网络安全规划等内容的认识有了一定程度的提高，为切实解决网络安全问题奠定了基础。本章将对网络安全实施进行探讨。

网络安全实施是解决网络安全问题的一个关键步骤，只有网络安全实施到位了，网络安全问题才有可能得以有效解决，否则所做的规划、设计都将失去意义。网络安全实施涉及的范围相当广泛，包括硬件设备、网络系统、网络软件、系统软件、应用软件、人员管理、规章制度以及网络安全教育和培训。

从总体上来说，网络安全问题就是人的问题，因为网络安全问题都与人有关，哪怕是硬件设备被盗或是发生火灾，都与人为的疏忽有关，最终解决网络安全问题的也是人，所以网络安全实施应该以人为中心，围绕这个中心来思考和解决网络安全中遇到的各种网络安全问题，网络安全问题才能得到有效的解决。网络安全实施中应该包括所有与计算机网络有直接关系和间接关系的人的管理，上至企业负责人，下至普通职员，甚至是打扫卫生的人员，除此之外，还有企业的外来人员，这类人员包括供应商、客户、企业合作伙伴以及其他人员。总之，只要可能和企业网络发生关系的人，都应该得到有效的管理，只有这样，网络安全问题才能得到有效解决。

通过对本章的学习，读者应当充分掌握网络安全实施过程中的各个注意事项，避免因为疏忽造成安全漏洞，造成企业网络安全问题发生，给企业带来经济损失和其他的损失。特别是在网络安全实施过程中，千万不能忘记必须以人为中心，如果忽略了这一点，再好的规划设计都不会有好的效果。

教学重点

- 网络安全实施原则。
- 掌握网络安全措施。
- 熟悉保护网络安全的 7 个步骤。
- 备份重要数据。
- 敏感文件保护。
- 熟悉日志分析。

9.1　网络安全实施原则

网络安全实施中应该遵循的第一个原则就是以人为中心。不同的人员在计算机网络系统中扮演不同的角色，需要充分认识这些角色可能对计算机网络安全造成的影响，然后采取有效措施消除负面的影响，增强正面的影响。

网络安全实施中应该遵循的第二个原则就是分步实施。计算机网络安全问题是一个系统性的问题，涉及很多的内容，想要一次性解决所有的问题是不可能的，况且，网络安全问题还是一个动态发展的过程，即使之前的网络安全问题已经解决，随着时间的推移，仍然会出现新的网络安全问题。所以，合理且有效的方法就是采取分步实施，把各种网络安全问题根据其重要性和紧迫性划分为几种类型，确定哪些问题需要及时解决，哪些问题可以稍后解决。

网络安全实施中应该遵循的第三个原则是科学化。网络安全问题通常存在多种形式，有的问题看起来好像可能性不是很大，发生的几率很小，有的问题好像听说的比较多，感觉要重要一些，也许这些是事实，不管怎样，我们最好不要想当然地进行猜测，而应该采取科学的态度，既然存在安全隐患，那么就要尽可能采取有效措施，防范安全问题的发生。

网络安全实施中应该遵循的第四个原则是以需求为导向。要解决网络存在的所有安全问题几乎是不可能的，更何况有些安全问题，我们可能根本就不知道是什么，就算我们能把所知道的安全问题全部解决，但是这可能也会需要巨大的费用，而且这样的网络在使用上可能也会有非常大的麻烦，所以解决网络安全问题时，需要根据网络的结构特点、用途等，有所重点地进行。

9.1.1 网络安全策略

解决网络安全问题的最重要部分是要精确实施公司的网络安全策略。我们必须能对该策略进行分析，并想出具体办法在实际的网络中应用它。但什么是网络安全策略呢？我们为什么要创建它？网络安全策略应该包含哪些内容？

1. 创建网络安全策略的原因

安全策略能提供很多好处，确实值得花费时间努力来开发它们。网络安全策略是网络安全的蓝图或体系结构规范，所以它必须是精确的和完善的。下面是开发网络安全策略的一些原因。

（1）提供一种程序来审计现有的网络安全；

（2）为实施网络安全提供一个全面的安全架构；

（3）定义哪些行为被允许，哪些行为不被允许；

（4）经常能帮助该机构确定需要哪些工具和步骤；

（5）帮助表达关键决策人员之间的一致意见，并定义用户和管理员的责任；

（6）为处理网络安全事件定义一个流程；

（7）实现全局性的安全实施并执行，计算机安全现在已经是一个涉及整个企业范围的问题，各计算站点都应该遵守网络安全策略；

（8）如果需要的话，为采取法律行为奠定一个基础。

2. 网络安全策略应包含哪些内容

每个企业都应该结合自己的具体应用和网络环境制定一个网络安全策略。下面是一些建议的关键性策略组件。

（1）权威性和规范，这一部分规定谁负责安全策略，以及安全策略覆盖什么区域；

（2）允许的使用策略，这一部分规定公司对于其信息基础设施将允许什么和不允许什么；

（3）身份认证策略，这一部分规定公司将使用什么技术、设备或技术与设备的组合来确保只有被授权的个人才能访问公司数据；

（4）Internet 访问策略，这一部分规定公司认为哪些行为是对公司的 Internet 访问能力的合乎道德的和正当的使用；

（5）企业局域网访问策略，这一部分规定园区网内的用户应该如何使用公司的数据基础结构；

（6）远程访问策略，这一部分规定远程用户应该如何访问公司的数据基础结构；

（7）事件处理流程，这一部分规定公司应该如何组建一支安全事件响应队伍，以及制定事件发生时和发生后将使用的流程。

3．安全策略的三个不同级别

（1）开放的安全策略

公司在安全实施问题上倾向于网络和系统的开放性。他们希望在连通性、性能和易用性方面为用户提供更大的灵活性和自由度。

开放安全策略的认证：

- PAP（用于远程客户和分支机构办事处）
- 口令（企业局域网和拨号用户）

开放安全策略的访问控制：

- 广域网路由器和网关路由器中的访问控制列表
- 没有独立的防火墙
- 不加密

（2）有限的安全策略

公司采用了一种在网络连通性、性能和易用性方面的用户灵活性和安全实施级别之间谋求平衡。

有限制的安全策略的认证：

- 一次性口令（拨号和 Internet）
- 口令（企业局域网）

有限制的安全策略的访问控制：

- 在广域网路由器和网关路由器中的访问列表
- 在 Internet 和企业网之间的防火墙
- 路由认证（分支机构办事处和园区网之间）
- 在分支办事处链路上进行加密

（3）严密的安全策略

公司在网络安全实施上倾向于使用更严格的安全控制。他们喜欢使用一种安全性较高的默认策略，尽管这会限制用户的连通性并导致性能和易用性下降。这些公司被归类为一个具有严密的安全策略。

严密安全策略的认证：

- 数字证书（拨号，分支办事处和企业局域网）

严密安全策略的访问控制：

- 在广域网路由器和网关路由器中的访问控制列表

- 在 Internet 和企业网之间的防火墙
- 路由认证（分支机构办事处和园区网之间）
- 加密（拨号，分支办事处和一些园区网）

9.1.2 网络安全分步实施

随着企业网络规模的扩大，通常情况下，网络中既有路由交换核心设备，又有服务器及存储设备，网络管理员既要负责关键设备的安全，又要保证员工计算机的安全，只有这样才能谈得上网络的安全，所以工作量更大，那么我们如何保证企业网络安全呢？

1．网络安全范畴

对于网络管理员来说需要保证安全的对象主要有以下几个方面，每个方面都是网络安全的重要内容。

（1）服务器的安全

企业内部基本上都有一台到多台服务器，这些服务器负责企业网络内部计算机的 DNS 或 DHCP 服务，还承担企业 FTP 服务，WWW 网站服务。有的还具备代理功能和防火墙功能。这些设备的安全是不容忽视的，服务器出现安全问题将直接导致企业网络的彻底瘫痪。

（2）路由交换设备的安全

路由器和交换机负责企业内部网络的互连和路由工作，他是企业网络的核心枢纽。这些设备一般都是 24 小时×7 天工作的，一年 365 天不间歇。保障这些设备的安全也是让企业网络顺利运转的关键。

（3）员工计算机的安全

网络功能与优势就体现在员工计算机的协同工作上，所以说企业内部员工计算机的安全也是不容忽视的，可以说中小企业网络管理员最多最重的工作就在于负责企业内部员工计算机的安全上。任何一个病毒或漏洞的流行都将给网络管理员带来巨大的工作量。操作系统的重新安装可以说是家常便饭。

（4）其他设备的安全

除了上面所说的几个关键设备外，企业内部网络中肯定还存在着其他设备，例如 NAS，UPS 等，这些设备的功能也是非常强大的，在企业中的角色也是很关键的。所以其他设备的安全也要有所保障。

（5）相关设备的防火防盗

除了网络管理员对设备的安全防护，一些相关设备的防火防盗工作也要做好。例如机房中的各种线缆要定期检查，机房中的空调也要及时保养。企业应该制定严格的管理制度来加强对于这些设备的防火防盗工作。

2．从硬件入手

企业网络中的硬件包括路由交换设备，NAS 产品，服务器等。这些设备也是决定网络安全与否的首要因素。从硬件入手保障这些设备的安全是全公司网络安全的基础。主要手段包括以下几种。

（1）保存场所的安全

这些硬件设备保存场所的安全是非常重要的，我们不可能把这些设备随意摆放，如果企业有条件应该使用专门的机房来储存关键设备，并在机房安装安全的防盗门等保护设施。

保存场所也应该安排专人值班，避免非法人员接近关键硬件设备。

（2）电力支持的安全

任何硬件设备都需要电力系统的支持，对于一些偏远城市和地区，电力系统是不稳定的，经常会出现断电或者电压异常的情况，这很容易造成设备的硬件损坏，所以说为企业关键设备提供必要的电力支持也是非常重要的。我们可以通过安装合适功率的 UPS 不间断电源来实现电力支持和稳定电压的操作，让设备可以稳定高效的运行。

（3）设备使用上的安全

除了硬件防护和电力支持外，设备使用上的安全操作也是非常关键的，很多用户都不太注重使用上的安全，认为硬件设备很皮实，不是那么容易坏的，这点是一个很大的误区。一般来说服务器，路由器，交换机的重新启动和关闭都需要通过软件的方式实现，而不是人为的关闭电源。服务器通过系统的重新启动命令实现，路由器交换机也通过管理界面中的 reboot 命令解决。

最为关键的就是 NAS 设备了，如果随意地关闭电源，那么 NAS 设备中数据的重组是非常消耗时间的，可能需要好几天才能恢复正常运行；另外随意关闭 NAS 设备电源很有可能造成数据的丢失和损坏。UPS 设备的使用也要特别注意，不能够频繁地充放电，也不能选择功率太小的 UPS 设备，这都将大大减少设备的寿命。

（4）设备冗余是关键

一般来说企业网络安全是建立在内部网络的正常运行基础上的，设备长期不间断地运行难免会出现这样或那样的小问题，这时设备的冗余就是关键了。通过设备的冗余可以保证服务不间断而设备的交替运行，让企业网络更加稳定。

设备冗余主要包括网络线路的冗余——例如用一个 ADSL 线路作为网络出口线路的备份，如果主要出口线路中断则用 ADSL 临时提供出口带宽；服务器冗余用两台服务器提供两种服务，这样每个服务都由两台服务器提供，例如 DNS 服务，WWW 服务，这样当一台服务器负载加大或停止服务的情况下，另一台可以马上接管工作；磁盘的冗余可以说是最常见的设备冗余工作了，它保证即使有一块硬盘出现错误，保存在其上的数据也将完好无损。

3. 从软件入手

除了上面所说的硬件安全，中小企业网络的安全还需要从软件入手。软件主要包括 Windows 系统下的应用软件，Linux 系统下的应用软件以及路由交换设备中的 IOS 软件设置。

（1）Windows 系统下的应用软件

Windows 系统是大家最常用的操作系统，我们可以通过安装第三方防火墙和杀毒软件来提高系统的安全性。毕竟很多时候系统漏洞补丁不能及时更新，这时第三方防火墙可以帮助我们阻挡漏洞病毒的入侵，杀毒软件也可以提高系统的运行效率，将病毒清除出系统。当然杀毒软件的病毒一定要及时更新，否则将起不到任何安全防护作用了。

（2）Linux 系统下的应用软件

一般来说中小企业员工使用 Linux 系统的机会不多，大部分都是在服务器上安装 Linux，这时就需要我们这些网络管理员安装提供工作效率的软件了，例如 Linux 下的系统优化和服务优化软件，帮助服务器更好地提供服务。

（3）路由交换设备中的 IOS 软件设置

路由交换设备的软件防护对大家可能比较陌生，很多人认为路由交换设备安装完毕就可以直接使用了，不用什么设置。其实这种想法是错误的，在实际工作中我们可以通过设置路由交换设备的 IOS 配置来提高企业网络的安全系数。主要手段包括访问控制列表的设置，通过访问控制列表 ACL 来防范黑客的入侵和病毒的传播，还可以更好地管理企业网络，让员工的网络访问权限划分得更加明确。

路由策略的设置，通过路由策略可以提高企业网络访问的效率，将各个部门的出口线路进行规划，为企业网络出口提供多条备份线路；虚拟局域网的设置，通过 VLAN 虚拟局域网帮助企业更好地管理网络，将部门与部门的计算机隔离，防止网络的非法访问。

4．从系统入手

如果说软件防范可以提高企业网络的安全性，那么从操作系统入手提高网络安全也是不容忽视的。

（1）漏洞补丁莫忘记

一般来说企业内部计算机都是采用的 Windows 操作系统，该系统的漏洞和缺陷还是比较多的，基本上每月微软公司都会发布漏洞补丁，如果不及时更新这些补丁程序的话，病毒和黑客很容易实现入侵目的。当然我们可以通过 Windows 系统自带的 Update 组件来完成自动更新工作，减少了我们的工作量，也让补丁可以及时下载和安装。

第一步：在所有员工计算机系统桌面的“我的电脑”上单击鼠标右键，选择“属性”。

第二步：在系统属性窗口中找到“自动更新”标签，将自动更新设置为“自动（推荐）”，然后设置其为“自动下载推荐的更新，并安装它们”，选择一个安装时间段即可。

第三步：确定完毕后我们的系统就将在每天固定时间自动连接 Windows Update 自动更新站点查看是否有更新信息了，如果有将自动执行下载和安装操作。

（2）系统账号要牢靠

很多员工都对系统账号的安全性不太重视，认为保持空密码或者弱口令输入着方便。其实这使得系统的安全性大打折扣。黑客和病毒可以对空密码或弱口令进行扫描，实现入侵的目的。所以说我们要将没有用的账号删除或禁用，为自己经常用的账户，特别是具备管理员权限的用户设置一个复杂的密码。设置密码的步骤如下。

第一步：通过任务栏的“开始”|“运行”，输入 CMD 后回车进入命令行模式。

第二步：在命令行模式中通过 net user 命令来查看当前本机存在着哪些账户。

第三步：再通过“net user 账户名 密码”来实现修改密码的操作，例如我要修改 administrator 账户的密码为 admin123654，那么执行“net user administrator admin123654”命令即可。

（3）服务是关键

系统中的服务也是安全的关键，一方面我们要将没有用的服务关闭，例如 messenger 和 remote register 服务；另一方面我们也要优化已经开启的服务，让他们尽量少占用系统资源。

对于服务器来说，系统服务则更加重要，例如服务器经常提供的 WWW 服务和 FTP 服务，这些服务对应的程序或多或少都会存在着漏洞，这些漏洞的弥补也是非常关键的。例如用 serv-u 程序建立的 FTP 服务器容易受到 Ddos 攻击，而用 IIS 建立的 WWW 服务在解析 ASP 语言时经常出现问题。这些程序漏洞都是可以通过安装服务补丁来解决，所以我

们要保证网络安全就要注意服务漏洞的补丁安装工作。

（4）组策略，用户权限齐上阵

如果企业自身需要对内部员工进行规范处理，分配合理权限的话，我们还可以通过设置组策略和用户权限分配，甚至是添加一个域来解决。组策略可以统一管理域中的所有计算机，域账户管理则可以针对不同的用户分配不同的权限。这些都能很好地提高企业内部的网络安全。

5．从制度入手

对于我们这些网络管理员来说主要责任就是管理好公司网络，保证其正常运行。不过网络上的应用软件和服务太多了，有的能够帮助我们企业运转，而其他则对我们公司的网络平稳运行有很大坏处，例如容易引起病毒的传播，黑客的入侵，系统的崩溃，数据的丢失等，虽然从技术手段上我们也可以阻止这些问题的发生，但是俗话说网络三分技术七分管理。只有制定合理有效的网络管理制度来约束员工，这样才能最大限度地保证企业网络平稳正常的运转，例如禁止员工乱用计算机，禁止利用工作时间随意下载软件，随意执行安装操作，禁止使用 IM 工具聊天等，所以说网络安全第四步就是从制度入手。

网络管理员不是网络维修工，许多网络的问题都是管理的问题，因此，网络管理员应该关注你的网络管理制度！作为一个企业的网络管理员我们不但要做到“攘外”——防止外部黑客以及病毒的侵袭，还要做到“安内”——管理好公司内部人员的越权操作，所谓是“无规矩不成方圆”，因此制定一套严格的管理制度是你轻松管理的“法宝”，也是保证企业内部网络安全的重要手段。

6．从网管自身入手

网络技术是没有止境的，不管一个网络管理员他自身水平有多高，如果他不能做到及时更新自己的知识，多看新技术书籍，多学习新管理经验的话，他就不算是一个合格的网络管理员。所以说网络的安全与网络管理员自身素质和水平有很大关系，虽然巧妇难为无米之炊，但是有了好米不会煮也是问题。一个企业拥有一名够格的网络管理员会减少很多网络隐患，在网络运行与维护上也将达到事半功倍的效果。

因此网络安全的最后一步就是要我们这些网络管理员从自身入手多学习新知识，新方法来提高企业内部网络的安全。同时制度对于网管的要求也是必需的，有些企业的网络管理员在网络权限方面过大，自己拿企业的服务器干私活，自己拿企业的服务器当成娱乐工具，这些都是不对的。所以要保证企业网络安全对网络管理员自身的约束也是不可缺少的。

9.2　安全性设计过程

企业网络的安全问题，自始至终都是一个比较棘手的事情，它既有硬件的问题，也有软件的问题，但最终还是人的问题。在对企业网络的安全策略的规划、设计、实施与维护过程中，你必须对保护数据信息所需的安全级别有一个较透彻的理解。所以你应该对信息的敏感性加以研究与评估，从而制定出一个能够提供所需保护级别的安全策略。

同时，当一个企业中的每一个商业单元都需要来自某单一点的有效管理时，要求你在统一的安全策略中找到各单元之间的相关性。这样在制定安全策略时，可以在用户之间自

动地进行复制，大大减少所需时间，还可以保证系统的统一安全。当系统实施策略发生改变时，全面的策略特性可以除去手工改变每个策略的麻烦。

从整体情况来看，一个标准企业的安全策略应该能够随着客户基础的增长，管理系统可以进行相应地有效升级。这其中包括有各种各样的策略描述。

9.2.1 安全原则

如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和必须解决的一个重要问题。计算机网络建设、使用的过程中应遵循以下几个方面的原则，以最大限度提高网络系统安全性。

1. 技术型原则

（1）把用不着的服务和功能全都阻断或禁用

除极少数例外，已知的远程攻击手段都与系统中运行的服务有关。因此，只要阻断有关的访问通道或禁用有关的服务，就不会给相关的攻击手段留下可乘之机。最少的服务加最小的限权等于安全。

当然有些服务是必须或者不得不启用的，例如，如果想运行一个 Web 应用程序，就不得不启用诸如 IIS（Internet Information Server）之类的应用服务。因此，如果必须开放某项服务，请务必按有关的指导意见对它进行防护。

至于应用程序，因为它几乎总是独一无二的，所以安全性要取决于程序员是否具备良好的编程习惯。

（2）一定要设置口令字，要让它尽量复杂，并且要经常更换

口令字是最基本的安全手段——需要进行身份认证的软件产品几乎都具备这一机制，Windows 也不例外。在专业深透测试实践中，弱口令字几乎总是我们攻破网络的突破口。一定要设置口令字（千万不要把它留成空白！），而且要把它设置成不能被轻易猜中（建议 7 个字符以上，并且要包含字母和数字）。如有可能，不妨把多种身份验证手段结合起来使用。

（3）打好软件厂商发布的各种补丁，一个都不能少

有软件开发经验的人都知道，有些事迟早会发生。每当在微软的产品里发现一个漏洞，那些急于出名和扩大传播范围的黑客们通常会在 48 小时内在网上发布一个利用该漏洞发起攻击的工具。这意味着在遭受攻击之前，通常只有大约两天的时间去安装微软的补丁。这种攻防就是如此不容喘息，不及时打好补丁的后果就是被未知的黑客从网上攻破系统。

（4）只授予有关账户完成操作所需的最小权限

这是网络用户最容易疏忽的概念之一，也是我们容易加以利用并攻破其网络的漏洞。授权行为都发生在身份验证之后，这是为了确保低权限用户不会访问到敏感资源。让别人猜出一个弱口令字就已经够糟糕的了，但在渗透测试中，我们经常发现刚弄到手的低权限账户甚至有权去挂装一个包含着企业财务数据的共享卷。我们知道，了解企业整个 IT 环境里的所有资源并给他们加上适当的访问控制确实需要花费不少时间，但如果不这样做，企业的信息防线的整体坚固程度将等同于其中最薄弱的身份验证环节——口令字强度最弱的那个用户。

（5）建立纵深防御体系

完善的防御系统不应该只有一条防线。当外围防线被攻破时，应该有内层防线继续抵抗攻击。根据这一原则，你应该把系统单元部署成能够“各自为战”的形式。这样，即使某个阵地失守了，攻击者也不可能轻易侵入其他阵地。

2．管理型原则

（1）安全问题，人人有责

这是一个很明显的问题，即使集中了世界上所有的安全专家也不可能应付每天发生的所有黑客活动。要把信息安全责任落实到企业中的每一个人，只有这样才能有效地抓好安全工作。

（2）对信任关系加以限制

信息系统不是孤立的，基于 Windows 系统尤其如此。我们用来攻击 Windows 网络最有效的手段之一是先设法侵入一台本地管理员口令字强度很弱的域成员计算机，然后再利用各种技巧从这台计算机上把某个合法域用户的口令字弄到手，进而在这个域里获得一个立足点并设法侵入与这个域有信任关系的其他域。一定要认真审查建立的每一个信任关系，不管它是一个正常的 Window 域信任关系，还是一个保存在远程计算机的某个批处理文件里的口令字；扩大信任关系将加大安全风险。

根据这一原则，应该明确禁止用户重复使用已经用过的口令字。下面这种事我们见得太多了：在渗透测试中，先侵入了一个 Windows 系统并破解了一些账户的口令字，然后发现这些口令字还能访问这个网络里的所有其他系统——企业的内部电话交换系统、UNIX 数据库服务器系统、SNA（System Network Architecture 系统网络体系）网关等。

（3）要特别注意企业内部网络的外部接口

网上潜在的薄弱环节数不胜数，但你必须学会把注意力集中在最脆弱的环节，企业内部网路与公共网络的联结处（比如 Web 服务器）就是这样的地方。这类系统是企业的“对外窗口”，是展示企业产品和形象的场所，也是最容易遭受攻击的头阵地，所以这类系统上的防护措施应该按更高的标准实施才行。顺便提醒一句：企业的内部电话网也属于“对外窗口”。

（4）安全撤退

当一个系统的保密性、完整性或可用性受破坏时，应该让它“安全地”撤退——即有步骤地停止该系统的运行，避免损失进一步扩大。

（5）越简单的安全措施越实用

简单的系统要比复杂的系统更容易防护，事情越简单，出现错误或缺陷的机会就越小。这一原则的具体体现是专用化和模块化：系统或系统的组件应该只有单一用途，这有助于避免潜在的冲突或冗余导致的安全漏洞。但维持众多单一功能的系统有可能他们总体的维护成本迅速加大，所以应该在这一原则的指导下对系统的各有关功能做最合理的安排。

（6）根据现实情况进行风险评估

不要为追求安全性而影响企业的商务活动，也不要为追求商业利润而忽视安全工作。我们见过太多因安全策略不够严格而导致损失的事例。

（7）技术并不能保证你免遭社交手段的攻击

我的目标是各种技术性的攻击手段——黑客们需要拥有一台计算机并具备一些计算机

使用技能才能加以利用的软件漏洞。但我们见过和听说过的攻击事例中，有不少后果极为严重的攻击根本与技术无关。所谓“社交工程（social engineering）”是指利用人与人之间的交往和误导而获得非法授权的数据访问途径。我这里只能向大家提供技术保护手段，它们不能保护你免遭与技术完全无关的社交性攻击。大家应该通过良好的交流和培训教育使你们的企业免遭社交性攻击。

（8）要比敌人更了解你自己的平台和应用软件

知己知彼，百战不殆。要想有效地防范黑客对我们计算机的入侵和破坏，我们更应该对网络安全体系有一个全面的了解，在系统真的遭受攻击时能灵活运用所学知识去进行防御。

9.2.2 监视和控制

从技术角度解决网络安全问题的方法包括两种，即监视和控制。这和我们现实生活中的其他地方几乎是完全一样的，比如说银行，这是一个安全性要求很高的地方，在银行不但设置有监视摄像头，而且还采取了多种安全保护措施，为银行的安全提供了相当的保证。对于我们的计算机网络也是一样。

只要我们需要在企业的计算机网络上开展工作，让人们使用计算机网络，就有可能产生安全问题。这里同样采取监视和控制两种措施，首先对于操作人员在计算机网络上的操作，凡是可能发生安全问题的，全部进行监视记录，通过查看这些记录信息，可以判断计算机操作人员是否进行了非法操作；对于另外一些操作并非工作需要，而且还会带来安全隐患的，直接通过网络控制系统进行控制，禁止操作人员进行相关的操作。这样可以大幅度提高网络的安全性，尤其是企业内部网络的安全性。

1. 被动监视

被动监视是一种普遍存在的监视方式，比如我们通常所见到的摄像头的监视就是被动监视。它只有监视的功能，只是简单地将监视到的信息进行记录，并不根据监视到的信息产生任何动作。

被动监视有一定的好处和弊端，其优点在于因为它没有对监视到的内容进行任何的判断并采取任何动作，所以被监视者往往会忽视其存在，被监视的内容也就有较高的真实性，这些信息作为一些依据也就会具有较强的说服力。其不足是即使监视到具有严重破坏性的行为，也不能及时制止，防止破坏的进一步发生，将损失尽量减小。应该说早期的监视大多数是属于这种类型的。

2. 主动的内部防御

据有关资料统计显示，企业计算机网络的内部安全问题往往比外部安全要大得多，所以做好内部网络安全工作，对于整个网络的安全具有重要意义。对于内部网络中存在的安全问题具有一定的特殊性，首先，内部网络是网络管理人员完全可以管理的，也就是说整个网络系统都是处于可以绝对控制的，这对于管理者来说，是一个有利的条件；其次，整个网络系统需要提供给企业内部所有人员使用，因为这是工作的需要，既要保证人们可以充分地使用网络，又要保证没有非法操作的破坏，这是一个很难解决的问题。

主动的内部防御是解决内部网络安全问题的有效方法，简单地说就是通过技术手段和管理手段，严格规定和限制计算机操作人员进行非法操作，以避免其对企业内部网络的破坏以及内部信息资料的泄密。

3. 被动的外部防御

对于和 Internet 连接的网络而言，或多或少都会受到来自外部的攻击，对于这些攻击，我们几乎不可能知道是从哪里来的，更不可能对其采取任何的控制行为，当然，这些攻击者也可能并不知道我们的计算机网络系统的存在，而只是在网络上使用扫描工具进行扫描时偶然发现了我们的计算机网络，然后开始进行试探性的攻击。

被动的外部防御是解决这类网络安全问题的方法，也就是说我们无法控制攻击者，也无法避免被攻击，我们唯一可以做的就是增强我们的网络系统，采取各种技术手段并加强管理，使得各种安全措施都能够切实得到执行，这是我们对于外部攻击所能做的。

4. 主动监视

主动监视不但具有记录监视内容的功能，还能根据监视到的内容，并结合预先设置的程序，采取各种有利措施，防止非法操作的进一步执行。这种监视实际上就是将被动监视和控制功能结合起来的形式。

这种监视的优点在于不但可以记录非法操作内容，而且还能阻止非法操作，有的还会根据非法操作情况产生各种报警信号，对保护重要信息有很好的效果。缺点就是系统相对复杂，再有就是如果使用不当，容易产生误报的情况。

9.3　网络安全措施

为了保证企业网络的安全，我们需要在企业网络上采取各种各样的安全措施，这些措施可能很简单，可以由员工自己完成，也有的需要网络管理人员完成，那么我们需要采取哪些措施呢？下面我们对各种措施做一个简单的介绍。

9.3.1　容易的工作

如果曾经完成安装程序或为计算机设置打印机之类的任务，则执行这些工作只会有少量麻烦，通常可以由员工自己完成。

1. 安装和更新防病毒软件

防病毒软件容易安装，而且一旦运行，就会持续不断地检查以防止可能通过网络损害或破坏数据的感染。 但是要知道黑客也在不停地编写新的病毒，仅当防病毒软件知道如何发现最新的威胁，它才有效。 因此当安装防病毒软件时，请将它设置为自动下载更新以便捕捉新的病毒。 如果购买的新 PC 包含的防病毒软件有试用期限制，请在免费试用期过期时注册以便继续获得更新，或投资另一种产品。

防病毒软件的使用方法可以参考本书第 2 章的相关内容。

2. 使用软件更新工具

微软公司会提供免费的工具，可以用来更新软件以使它更安全。 例如，只需要单击几次鼠标就可将 Windows XP 或 Windows Small Business Server 设置为使用自动更新功能。 此工具可以让 Windows 自动联机以查找并安装最新的更新来应付安全威胁。 打开自动更新之后，就不再需要做任何进一步的工作。 软件将自行更新。 Microsoft Office 系统也具有自动更新工具。

设置自动更新 Windows 系统的方法可以参考本书第 6 章相关内容。

通过微软公司提供的 Microsoft Office 自动更新工具进行自动更新的操作过程如下。

（1）在 IE 中登录 http://office.microsoft.com，如图 9-1 所示。

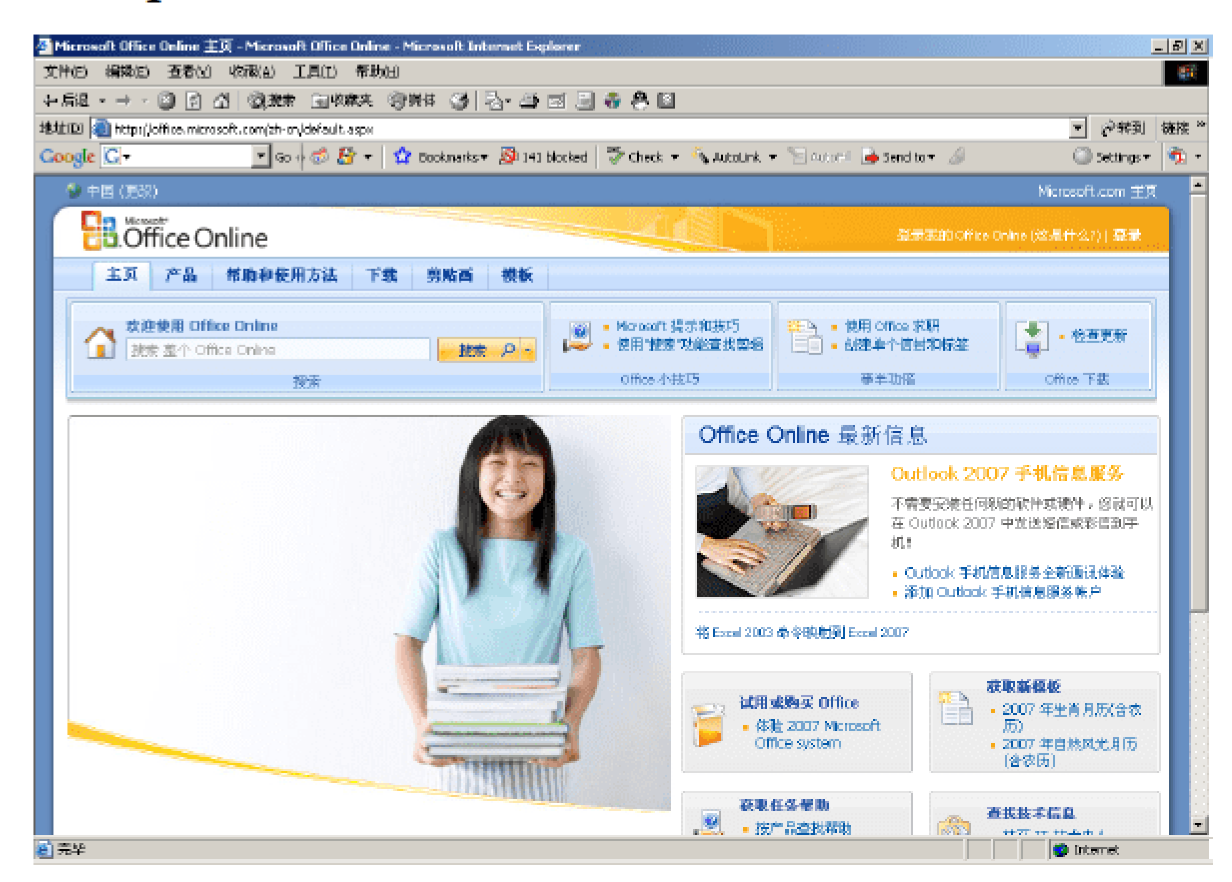


图 9-1　Microsoft Office 更新页面

（2）单击“检查更新”超级链接，出现如图 9-2 所示。

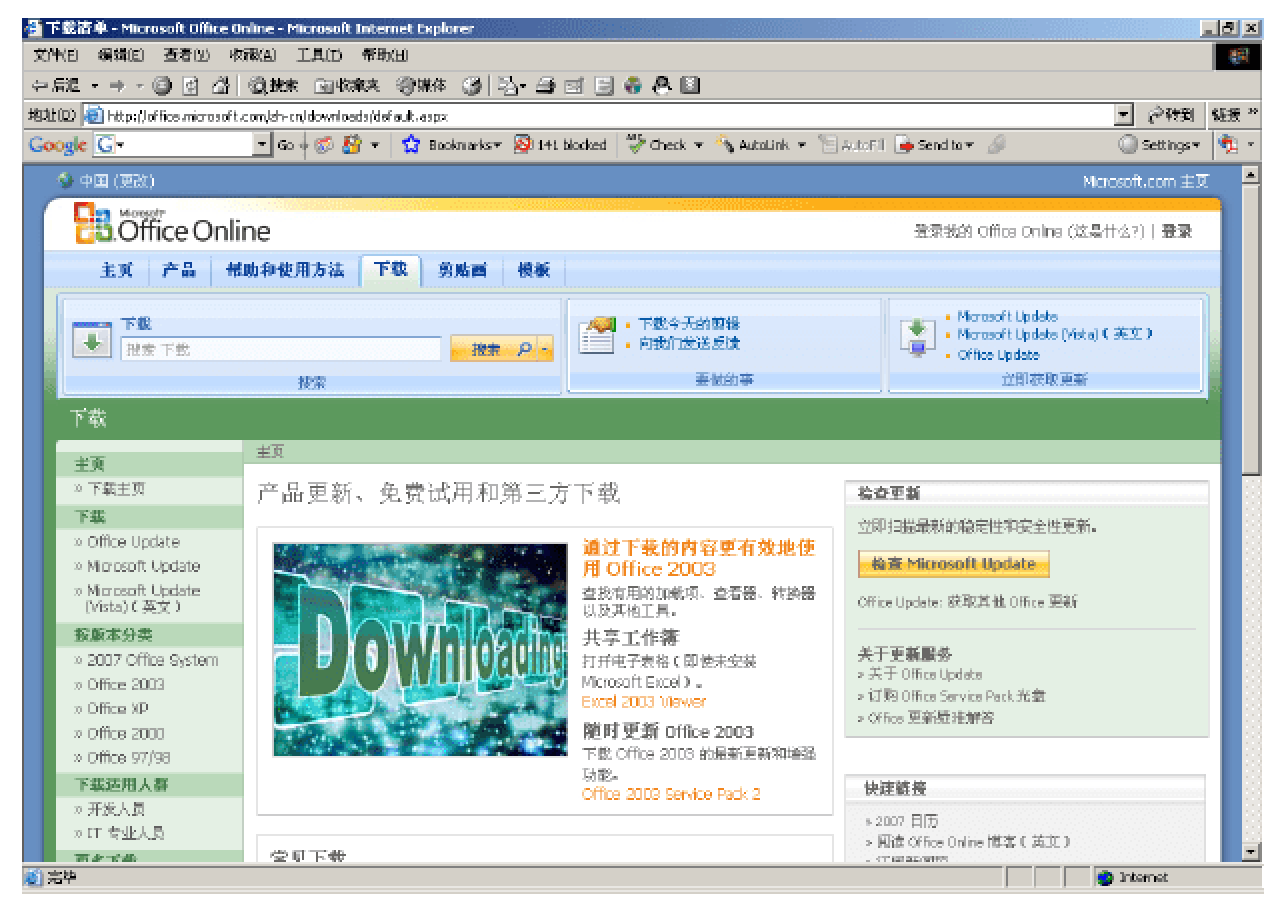


图 9-2　Microsoft Office 检查页面

（3）单击 Office Update，如果是第一次进行这样的更新，会出现如图 9-3 所示的“安全设置警告”对话框，提示需要安装微软公司的一个签名。



图 9-3　安全设置警告

（4）单击“是”按钮，完成签名的安全并开始运行，稍等一会儿，出现检测结果显示，如图 9-4 所示。

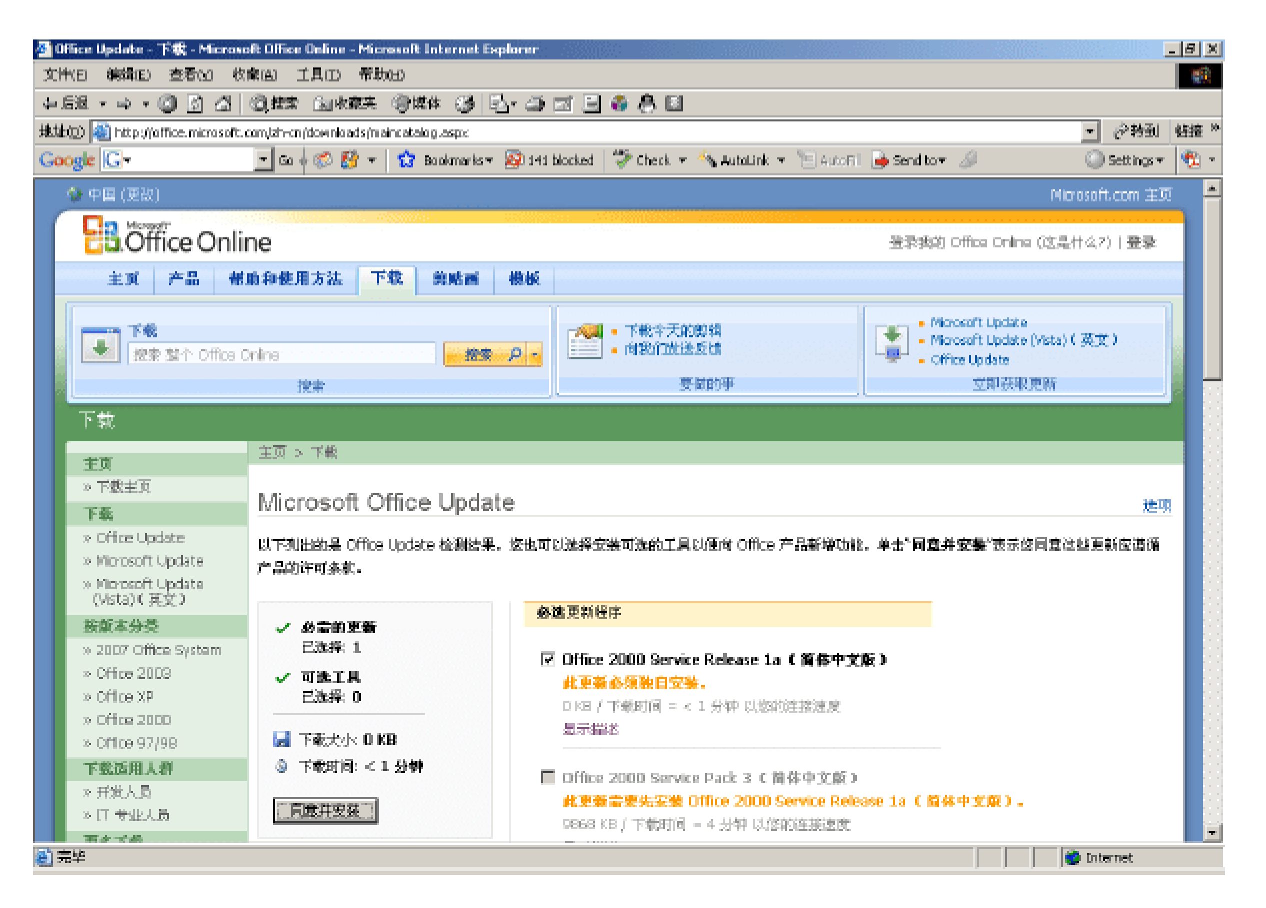


图 9-4　检测结果显示

（5）单击“同意并安装”按钮，出现需要更新内容的介绍信息，如图 9-5 所示。

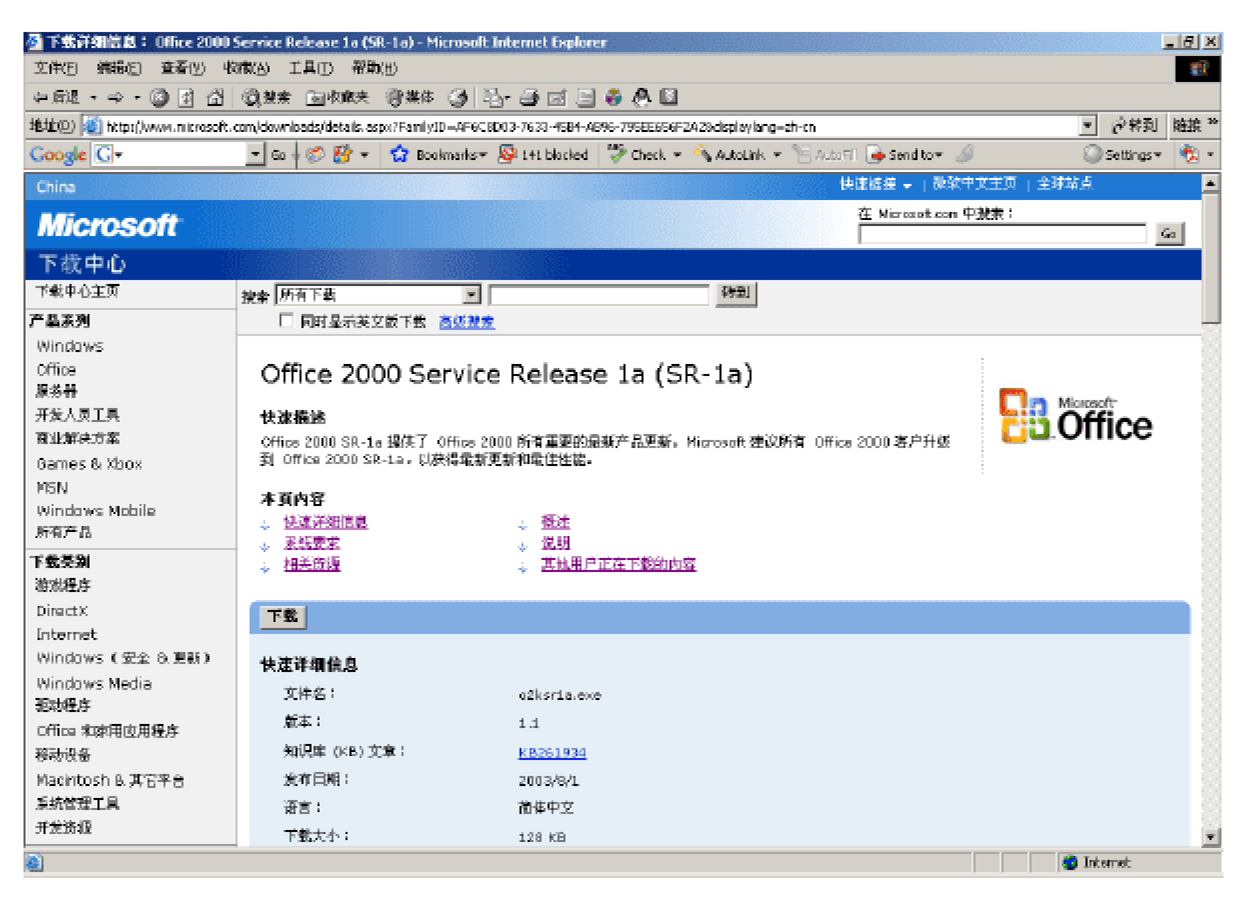


图 9-5　更新内容介绍

（6）单击“下载”按钮，将更新程序下载到本地硬盘，然后根据提示进行安装即可。

3．安装防间谍软件

请安装并定期更新防间谍软件，该软件查找试图收集密码和账号的秘密程序。Microsoft 提供免费的 Windows AntiSpyware 程序和恶意软件删除工具，可以使用它们除去 PC 中不需要的软件。

防间谍软件的使用方法可以参考本书第 6 章相关内容。

4．安装软件防火墙

防火墙检查进入网络的数据，如果数据不满足某个标准就会丢弃它。软件防火墙，如 Windows XP Professional 中内置的 Windows 防火墙，只保护运行它们的计算机，但为硬件防火墙提供良好的备用防御措施。打开 Windows 防火墙很容易。

开启 Windows XP Professional 中内置的 Windows 防火墙具体操作步骤如下。

（1）选择“开始”|“设置”|“控制面板”命令，出现如图 9-6 所示。

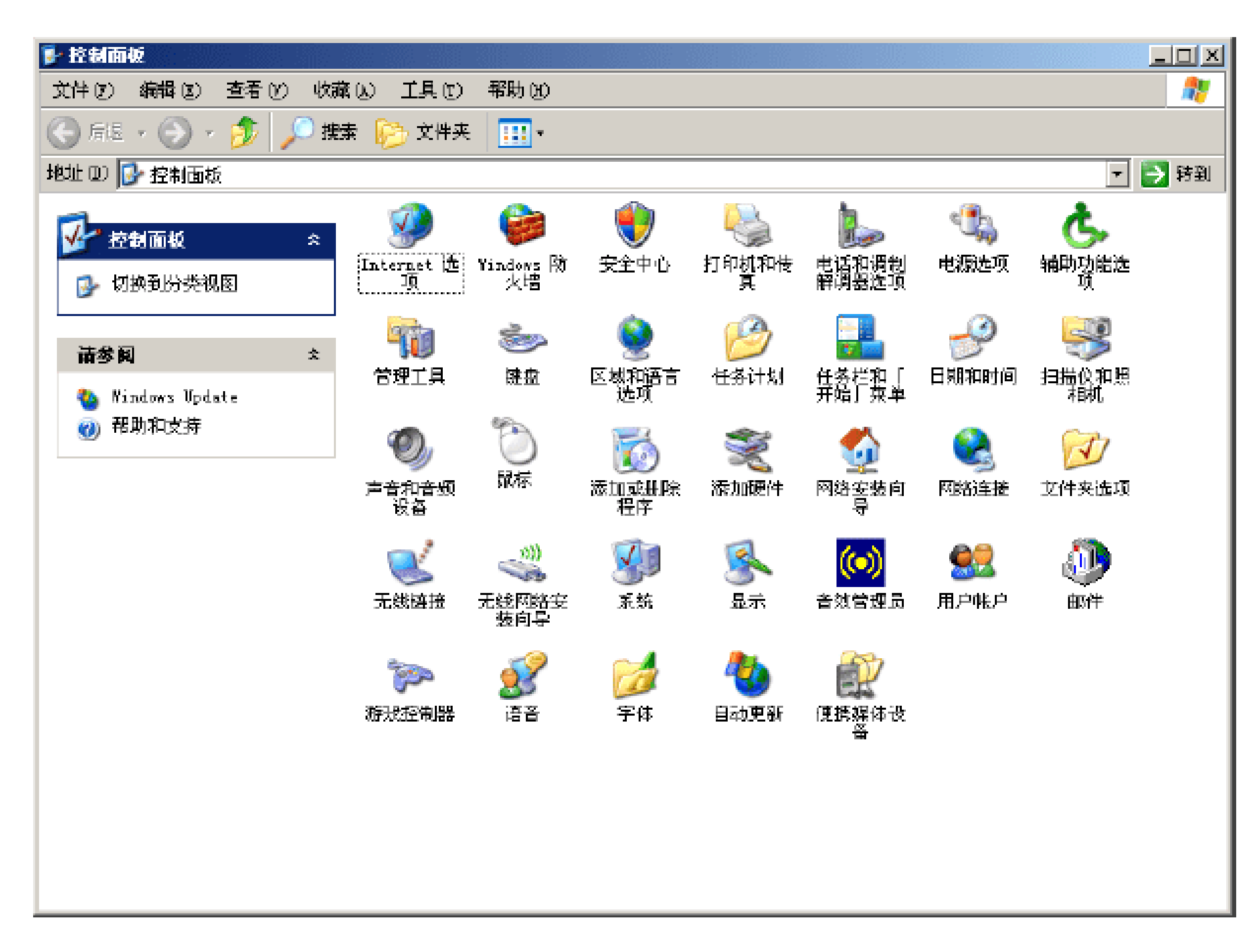
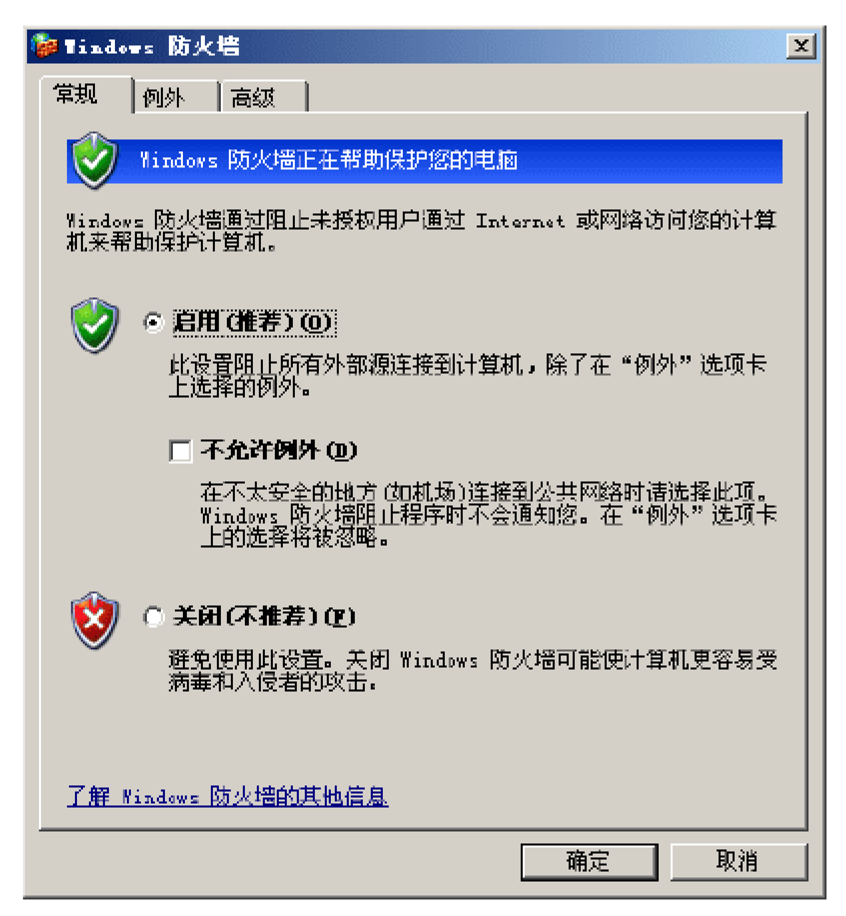
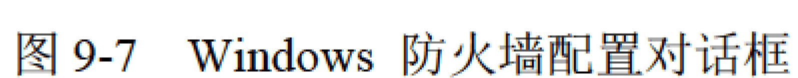


图 9-6 控制面板

（2）双击“Windows 防火墙”，出现“Windows 防火墙”配置对话框，如图 9-7 所示。

（3）选择“例外”选项卡，如图 9-8 所示，可以设置各种通信控制规则，包括按照程序和按照端口两种方式。





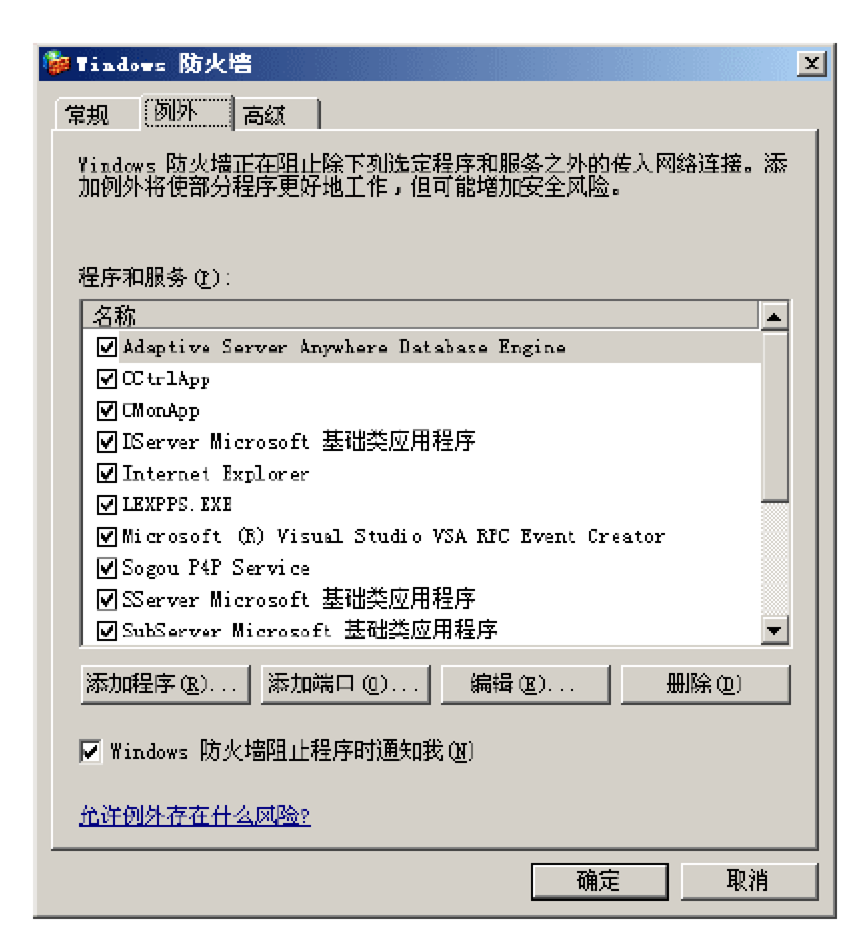


图 9-7 Windows 防火墙配置对话框　　　　图 9-8 防火墙规则设置窗口

（4）选择“常规”选项卡，选择“启用（推荐）”单选框，单击“确定”按钮，防火墙启用就完成了。

5．安装垃圾邮件筛选软件

垃圾邮件是未经请求进入收件箱的商业电子邮件，挑选垃圾邮件会浪费员工的时间。虽然大部分情况只是增添麻烦，但是当垃圾邮件包含打开会释放病毒的附件时，它就会带来风险。 另外，某些垃圾邮件属于“网页仿冒”类别，或欺骗收件人泄露密码以及其他可能使企业面临风险的有价值的信息。安装垃圾邮件筛选产品或配置内置的 Outlook 2003 垃圾邮件筛选器有助于显著减少垃圾邮件。

下面介绍快捷反垃圾邮件的使用方法。

（1）启动快捷反垃圾邮件主程序，主窗口界面如图 9-9 所示，界面类似于 Foxmail 邮件管理工具。

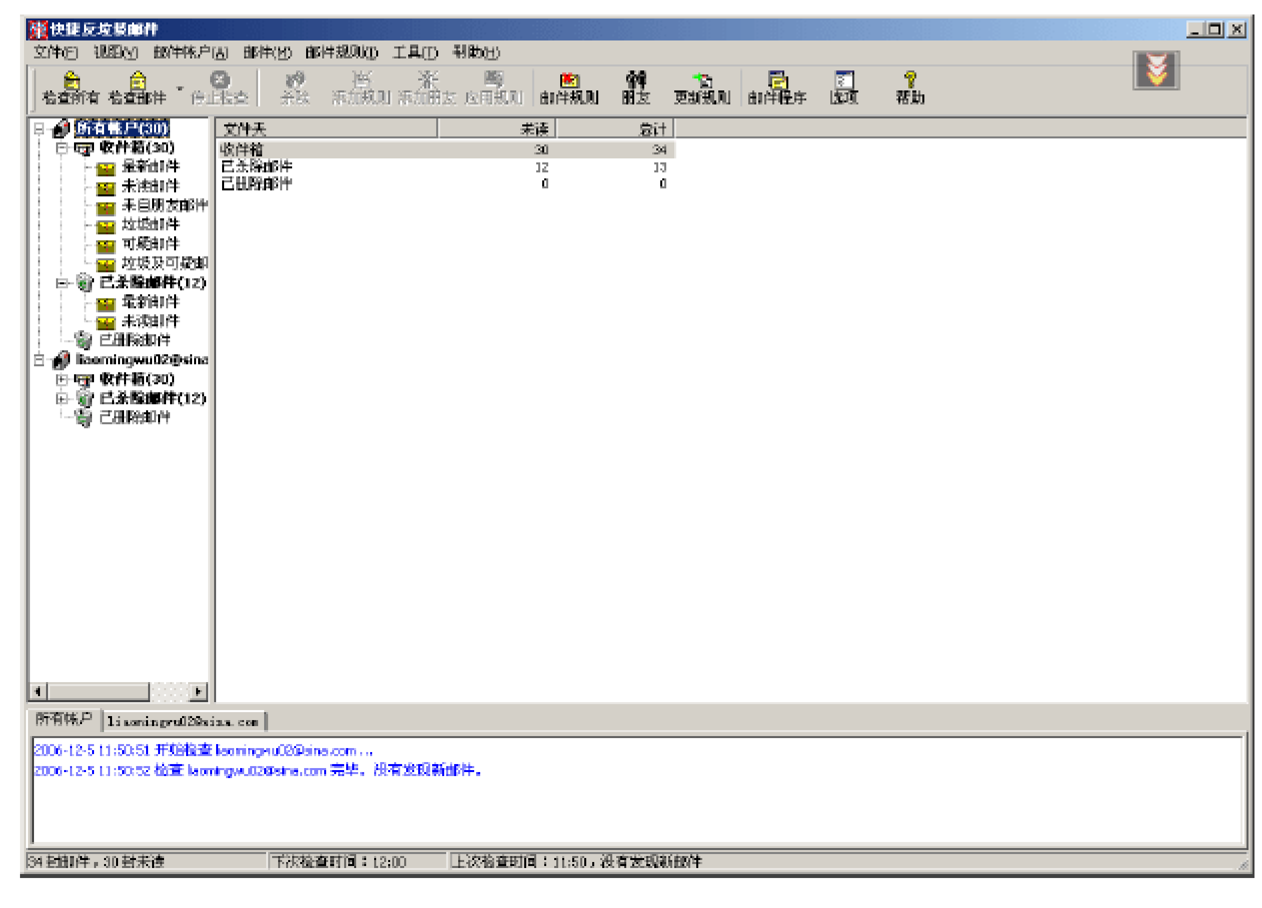


图 9-9　快捷反垃圾邮件主界面

（2）在窗口左边有不同邮件类型的树形列表，包括所有账户和单个账户两种方式。单击左边“所有账户”|“垃圾邮件”项，即可看到所有的垃圾邮件，如图 9-10 所示。

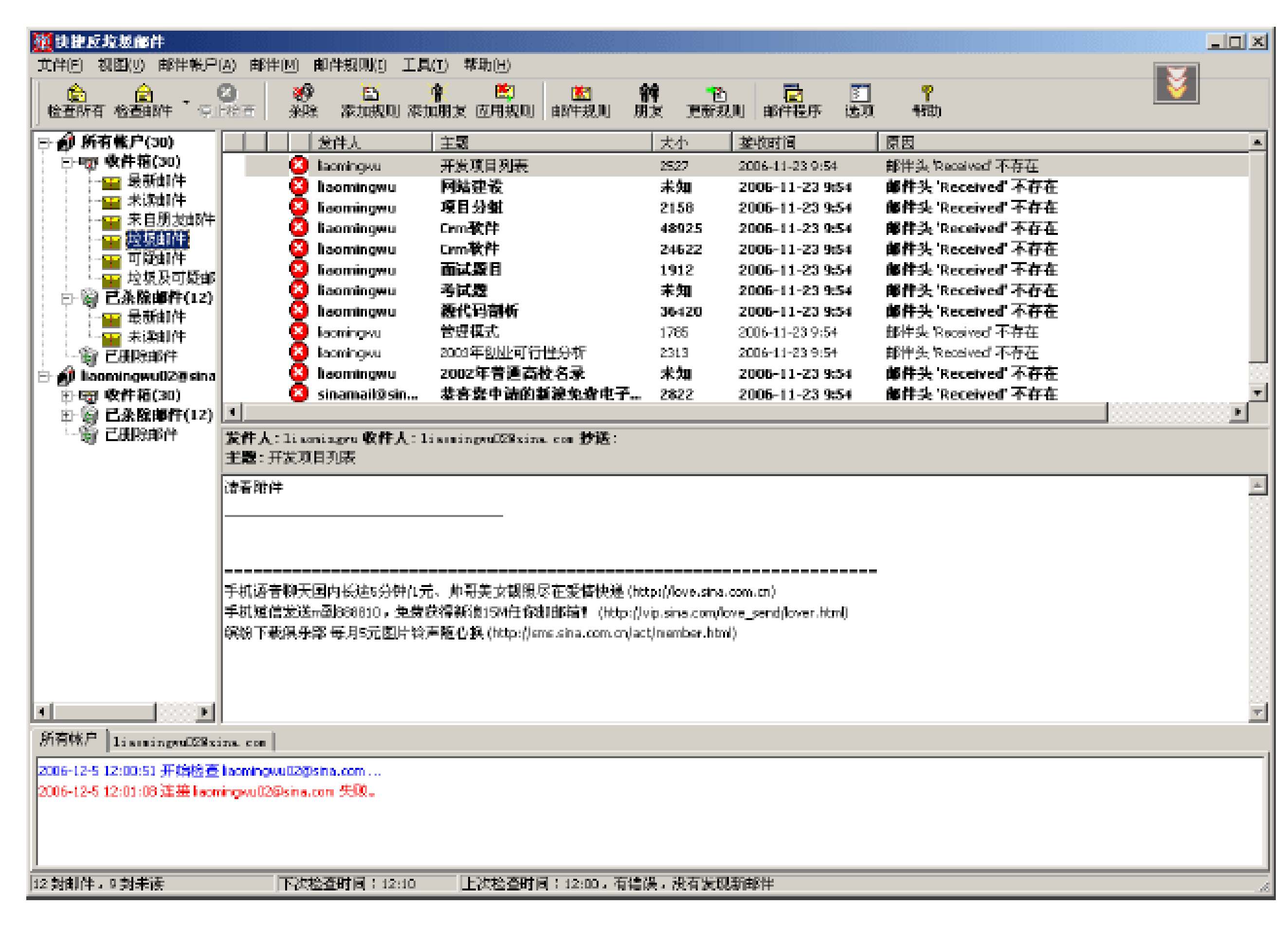


图 9-10　垃圾邮件显示

（3）单击左边“所有账户”|“可疑邮件”项，即可看到所有的可疑邮件，如图 9-11 所示。

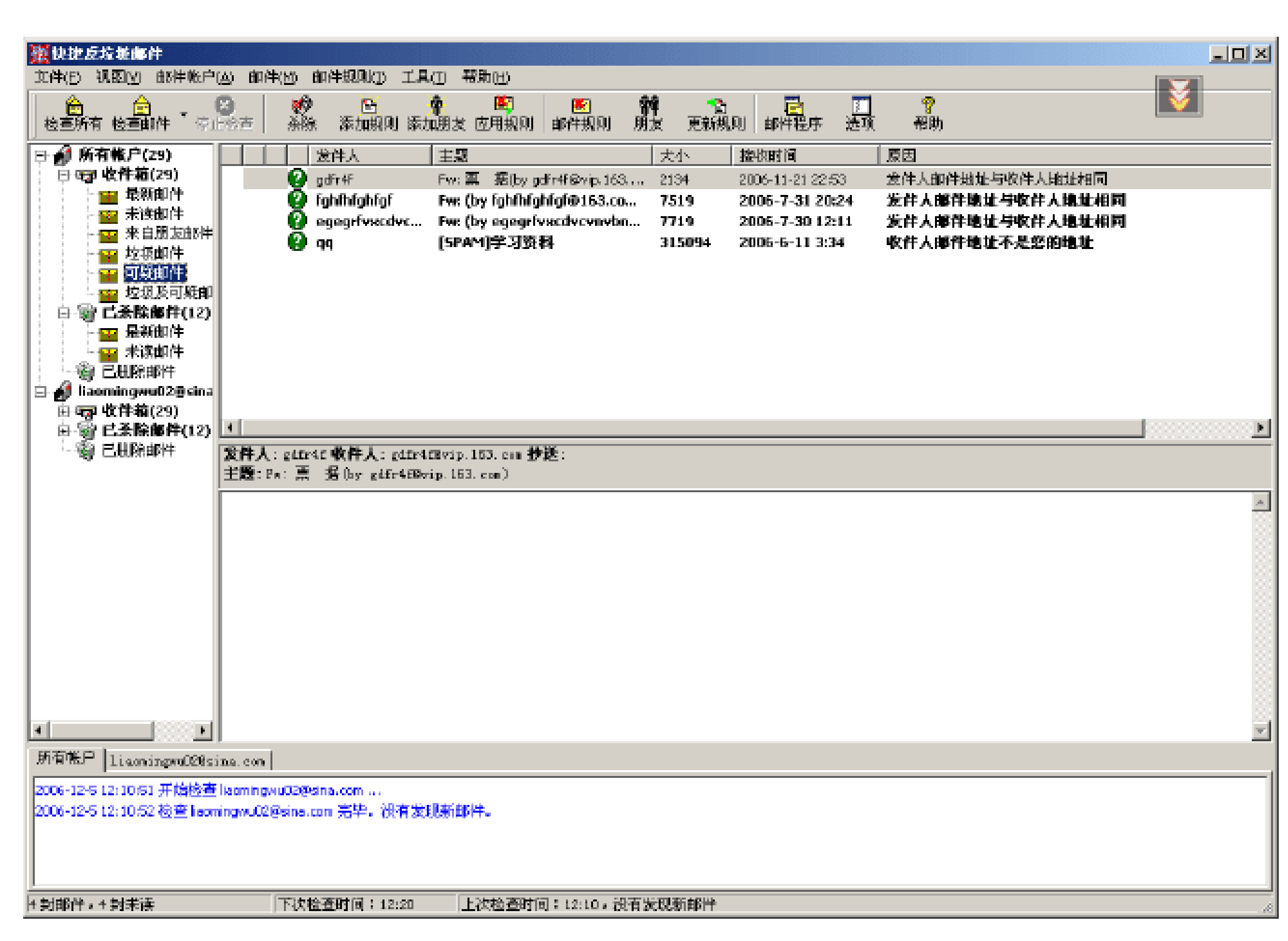


图 9-11　可疑邮件显示

（4）单击工具栏上的“邮件规则”按钮，出现邮件规则配置窗口，如图 9-12 所示。

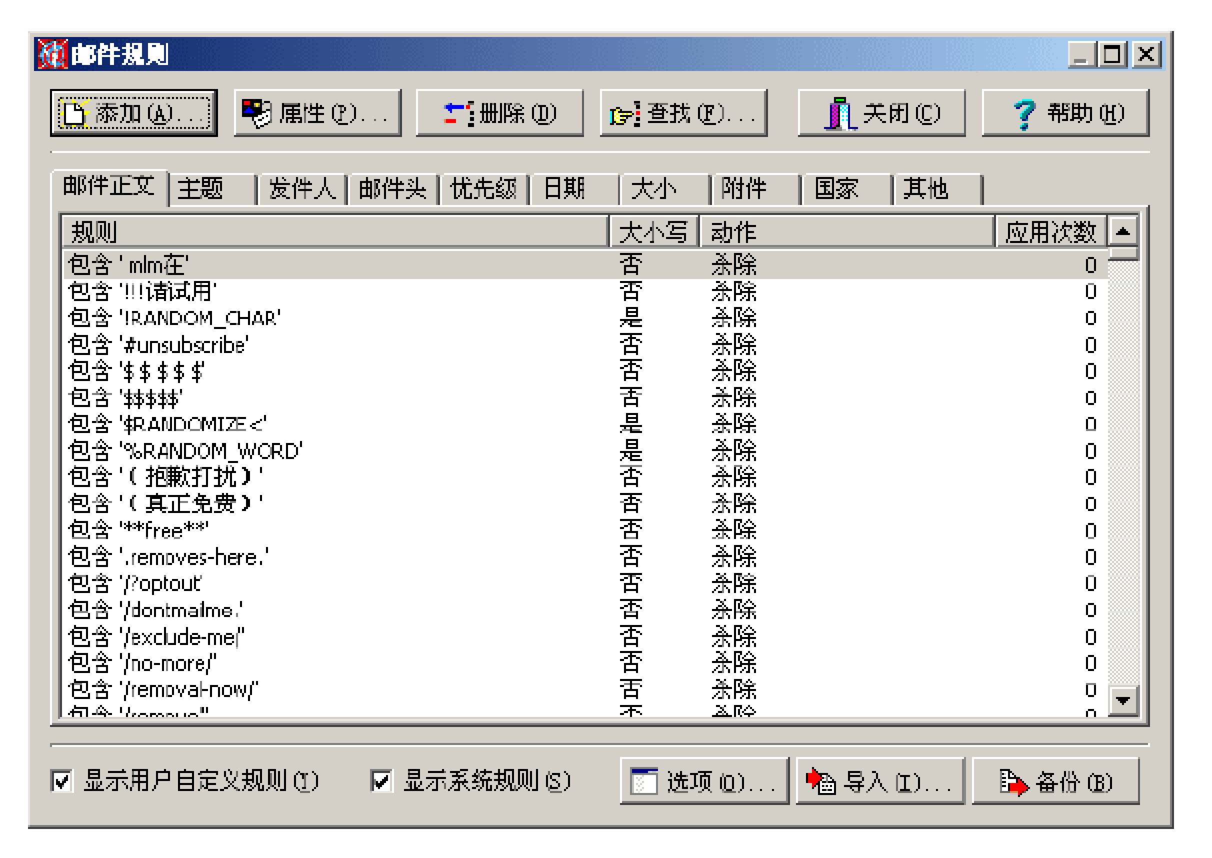


图 9-12　邮件规则设置窗口

（5）在“邮件规则”对话框中，提供了判断垃圾邮件、可疑邮件和垃圾及可疑邮件的判断规则，可以根据自己的需要进行灵活配置。

（6）除了上述功能以外，该软件还提供了其他的一些丰富的功能，使用该软件有利于减小垃圾邮件带来的大量时间浪费。其他功能的实际操作，留给读者作为练习。

9.3.2　较难的任务

这组任务可能更加困难。 它们需要更多的技术专业知识或持续管理安全策略和流程，通常由网络管理人员来完成比较合适。

1．限制设备访问

通过限制对服务器和网络设备（如路由器和交换机）的物理访问，可以提高安全性。 如有可能，请将这些机器移到加锁的房间，并确保只有指定在该设备上工作的人员拥有钥匙。这可以最大程度地减少不合格的人员篡改计算机或尝试“纠正”问题的机会。

禁止计算机外设的具体操作步骤如下。

（1）右击桌面上的“我的电脑”，从弹出的快捷菜单中选择“属性”命令，出现“系统属性”对话框，选择“硬件”选项卡，如图 9-13 所示。

（2）单击“设备管理器”按钮，出现“设备管理器”窗口，如图 9-14 所示。

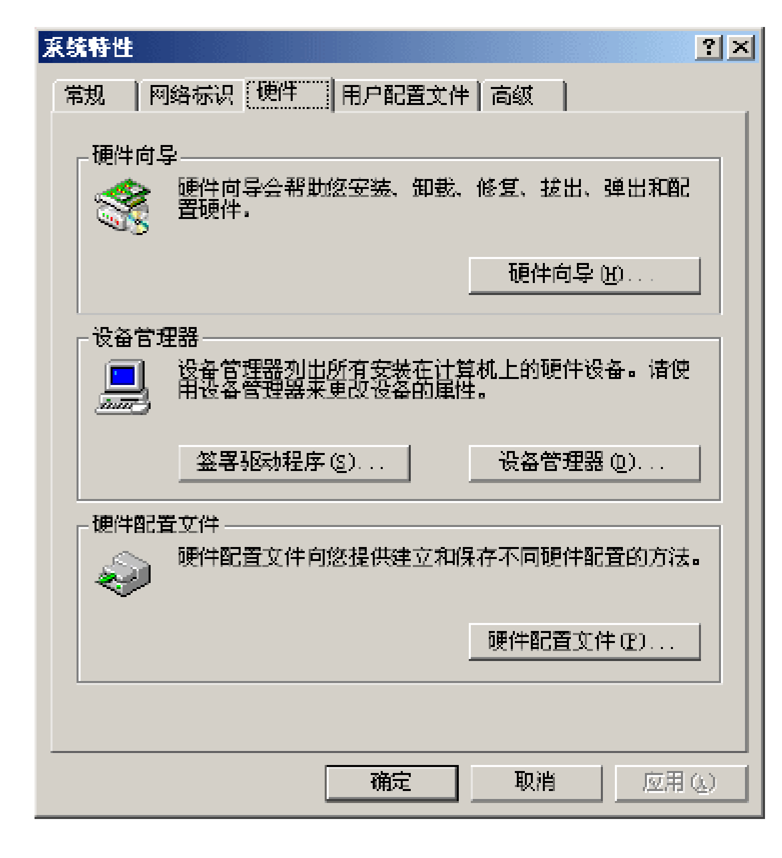


图 9-13　“系统属性”对话框

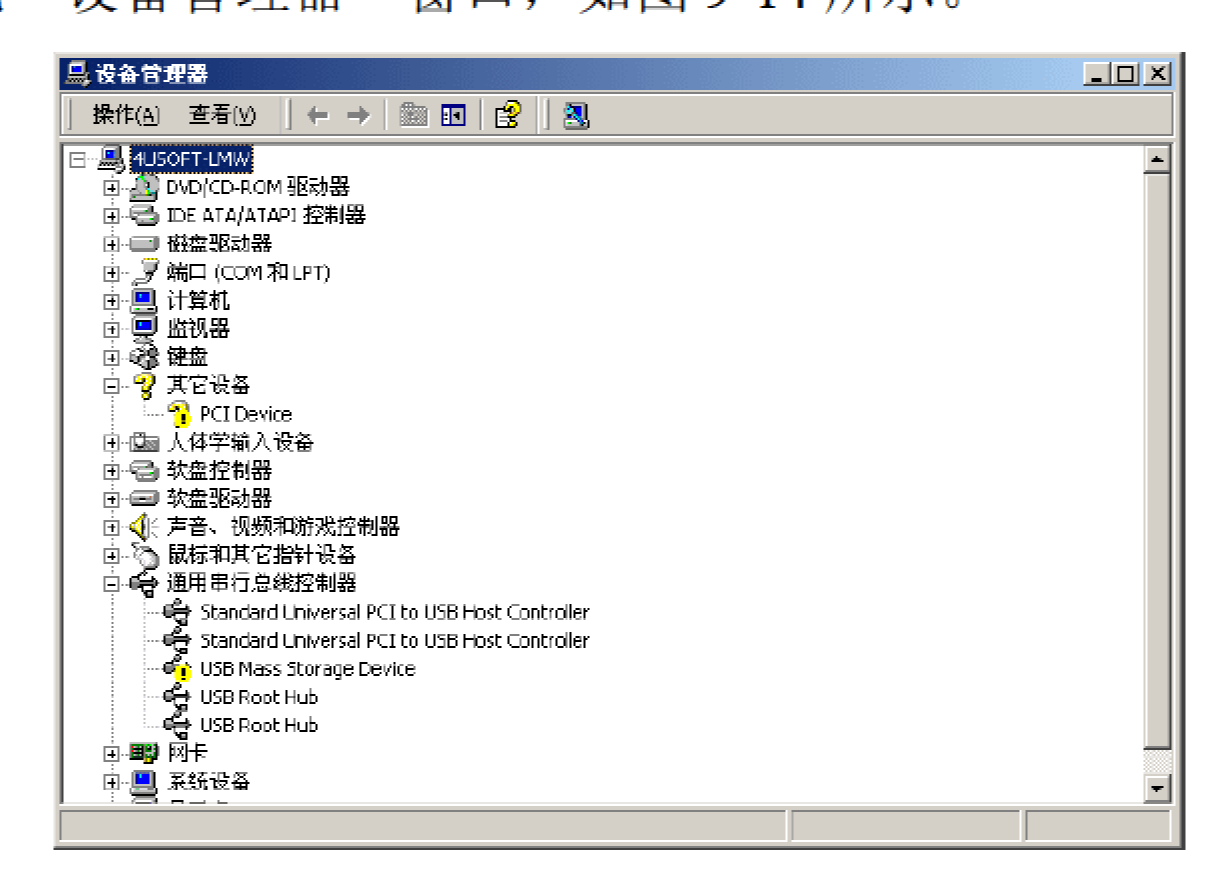


图 9-14　设备管理器窗口

（3）右击“端口（COM 和 LPT）”|“通信端口（COM1）”，在弹出的菜单中选择“停用”命令，出现确认对话框，如图 9-15 所示。

（4）单击“是”按钮，设备就被禁止，如图 9-16 所示。

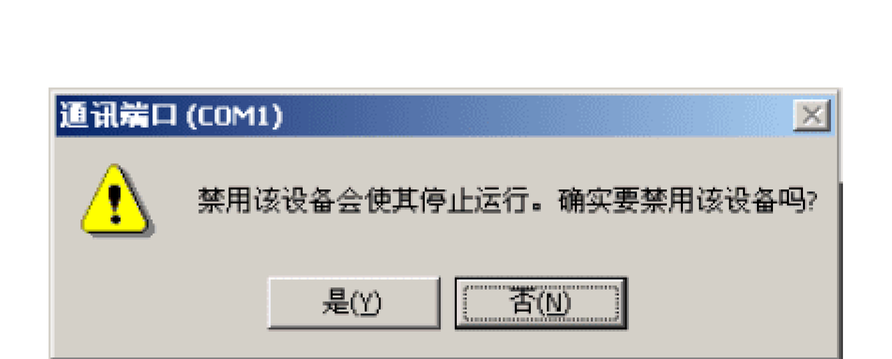



图 9-15　提示对话框

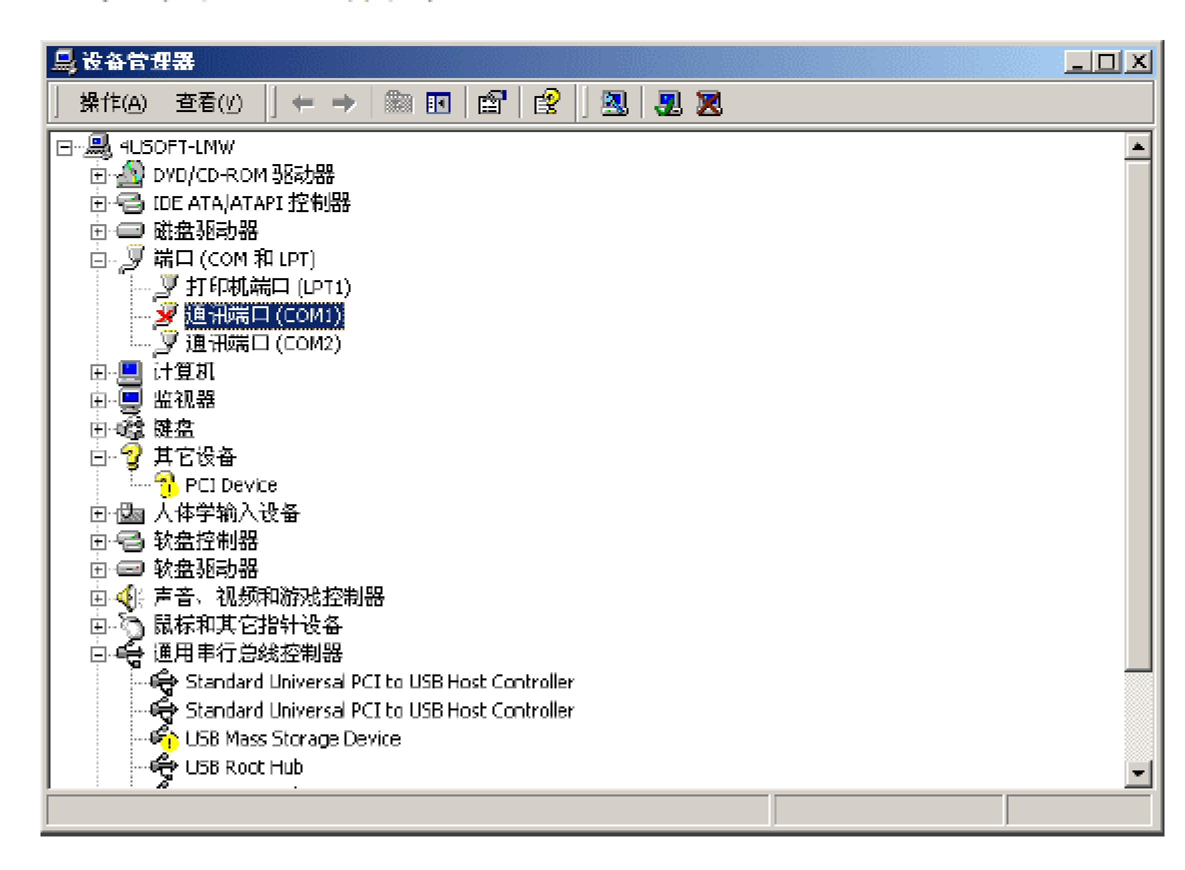


图 9-16　被禁止的设备状态

（5）采用同样的方法就可以启用或者禁止其他的设备。特别是以系统管理员登录系统禁止的设备，以其他账号登录后无法启用。

2．设置权限级别

可以使用 Windows Small Business Server 2003 给用户指定不同的网络权限级别。 不要给所有用户授予“管理员”访问权限，请只给某些用户授予对特定程序具有访问权限，并定义允许哪些用户特权访问服务器。 例如，可以给某些用户授予读取服务器上存储的某些文件但不能修改它们的权限。 应该只有网络管理员才能访问所有系统文件和服务。

3．删除离职员工的网络访问权限

消除离职员工登录网络的能力。 删除他们的访问权限和用户特权很容易，但是如果等待时间太长，就可能给心怀不满的离职员工损害或窃取文件的机会。

4．制订电子邮件和 Internet 使用策略

最新的研究表明，6% 的所有电子邮件感染了病毒或其他可能损害计算机的程序。 制订全公司的 Internet 使用策略，其中包括要求员工不要打开他们不想要的电子邮件附件的指示。 该策略还应说明危险的联机活动并禁止从网络上下载免费实用程序和其他程序之类的行为。 指示员工在接收到要求提供密码或账户信息的电子邮件时，不要泄露这些信息。

5．要求员工使用强密码

容易猜出的密码可能使未经授权的人员能够访问网络。 为了防止这种问题发生，安全策略应要求密码同时包含字母和数字。 而且，在要求定期更改密码的同时，避免要求员工过于频繁地更改它们。 如果他们觉得记住密码比较困难，他们可能记下密码并将它们粘贴在他们的显示器上，这使得其他人很容易闯入计算机系统。

9.3.3　请求帮助

这些任务技术含量不是特别高，但是可能需要考虑聘请计算机或网络顾问来处理它们，如果能够找到有相关经验的人员来执行，效果可能会好一些。

1．安装外围防火墙

软件防火墙保护安装它的 PC，而外围防火墙是插入并保护整个计算机网络的硬件设备。一个重要功能是它允许关闭网络端口。因为网络端口允许客户端计算机与服务器之间的通信，所以通过关闭不使用的端口可以增强网络的安全性并阻止未经授权的访问。此步骤实施起来比较困难，可能需要专家来帮助正确设置防火墙功能。

2．保护虚拟专用网络

将远程用户连接到公司的网络使他们能够检查电子邮件和访问共享文件。虚拟专用网络（VPN）可以让更安全地执行这种操作。但是，任何时候让自己的网络供外人访问都会存在很大的安全风险。可能需要请求安全顾问帮助，因为让 VPN 正确工作可能比较困难。

3．配置无线安全功能

在无线网络的无线电范围内的任何人都具有在网络上接收或传送数据的潜力。如果计划使用无线网络，则请求 IT 专业人士帮助以确保激活安全功能和正确配置无线加密和访问控制功能。

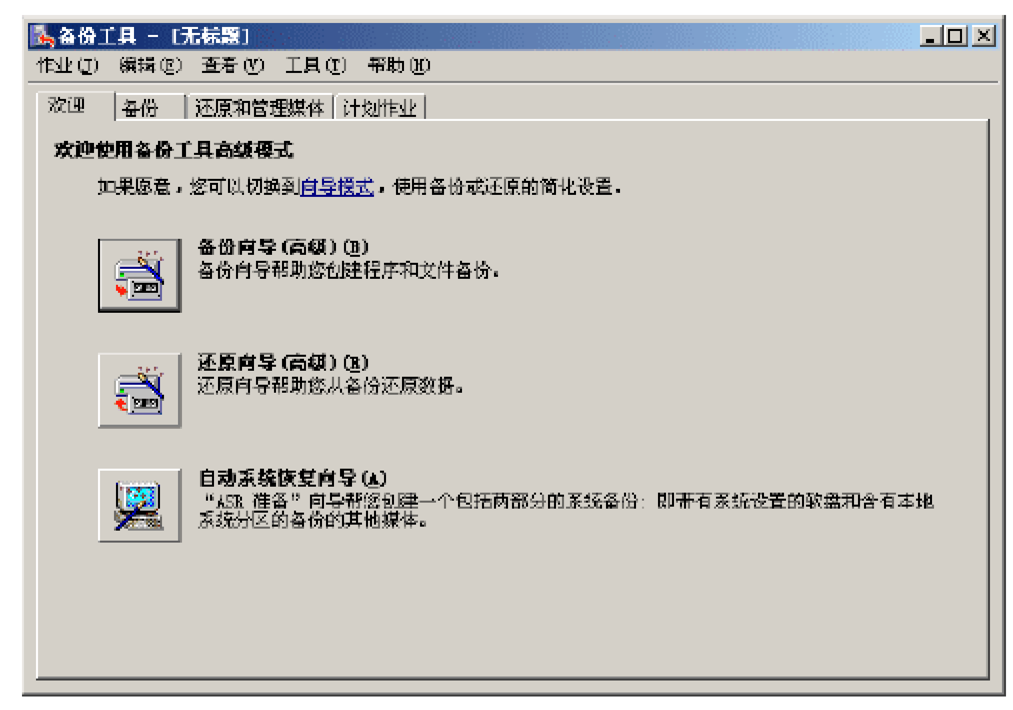
4．创建备份和还原过程

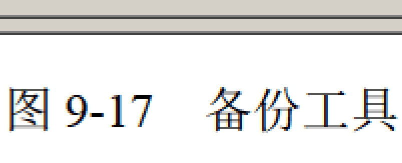
此任务可能与将数据文件刻录到光盘上然后将它保存在安全的地方那样简单。Windows XP 包含一个备份和还原数据的工具。如果需要让数据随时可用，应与 IT 专家合作，他可以用冗余配置的方式将硬件添加到系统中，这样每次保存文件的时候都会在另一个硬盘上保存那些文件的重复副本。这样，如果一个硬盘驱动器死机，则备份系统可以代替它并保持数据正常流动。应至少每周备份文件，并定期练习还原数据，这样做只是为了验证可以还原它们。

Windows XP 备份还原工具操作如下。

（1）选择“开始”|“程序”|“附件”|“系统工具”|“备份”命令，出现如图 9-17 所示。

（2）可以单击“备份向导（高级）”按钮对计算机上的指定位置的文件进行备份，也可以单击“还原向导（高级）”对以前做的备份进行还原，这两种操作都有向导的支持，比较简单，作为读者的练习。在此选择“备份”选项卡，如图 9-18 所示。




图 9-17　备份工具

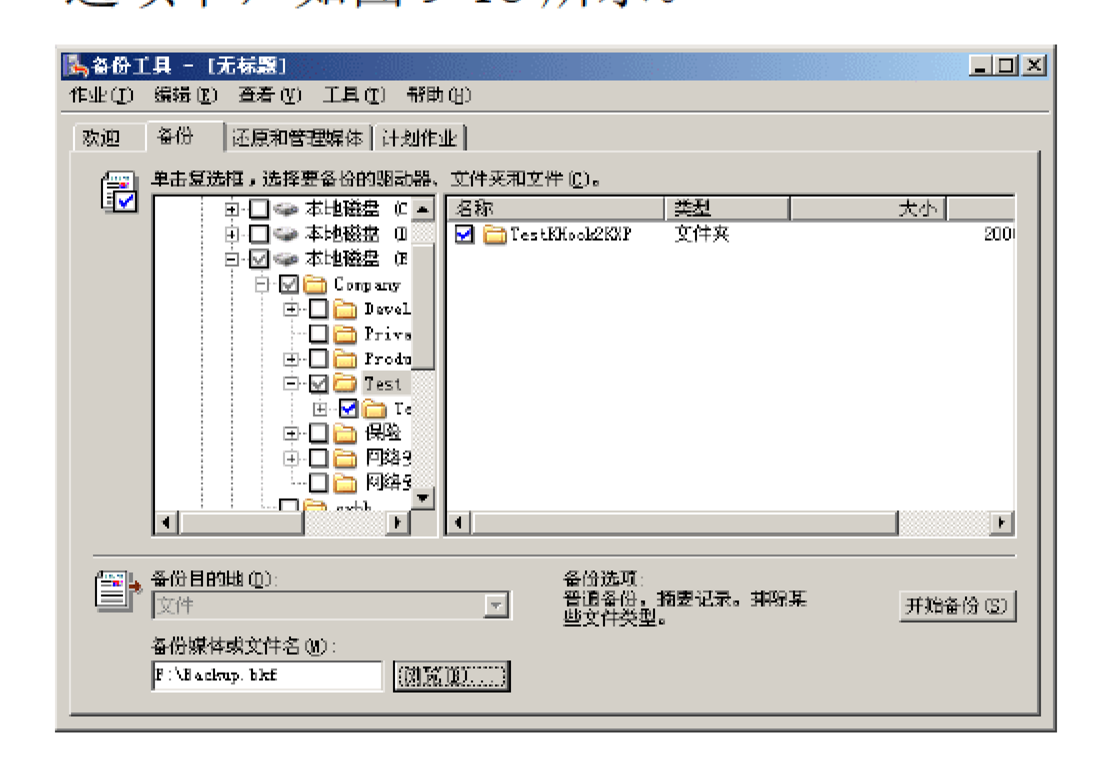


图 9-18　备份设置窗口

（3）首先在窗口左边的树形列表框中选择需要备份的文件夹，只需要在列表项前的复选框选中即可，其次单击“浏览”按钮设置备份文件路径和文件名，最后单击“开始备份”按钮，出现如图 9-19 的“备份作业信息”对话框。

（4）单击“开始备份”按钮，开始进行备份，备份完成后，出现结果提示框，如图 9-20 所示。

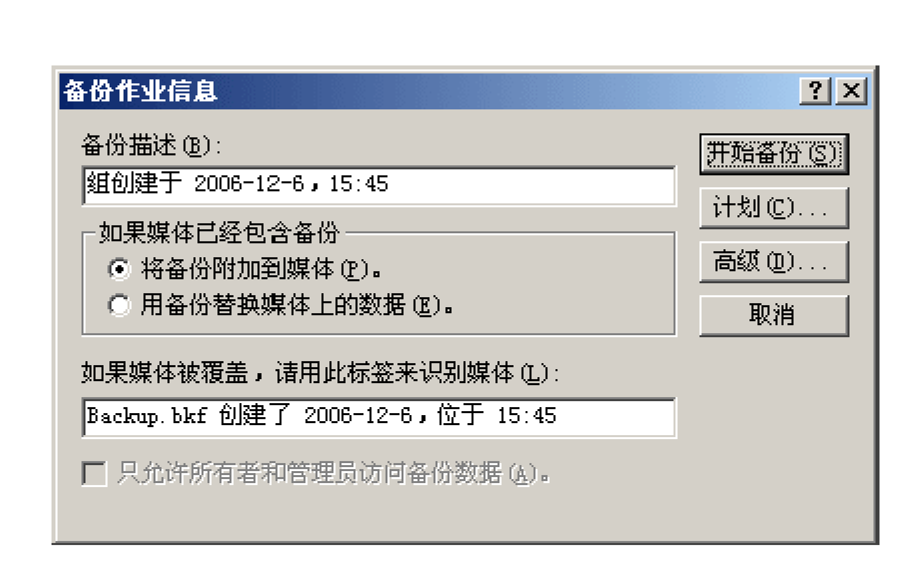


图 9-19　“备份作业信息”对话框

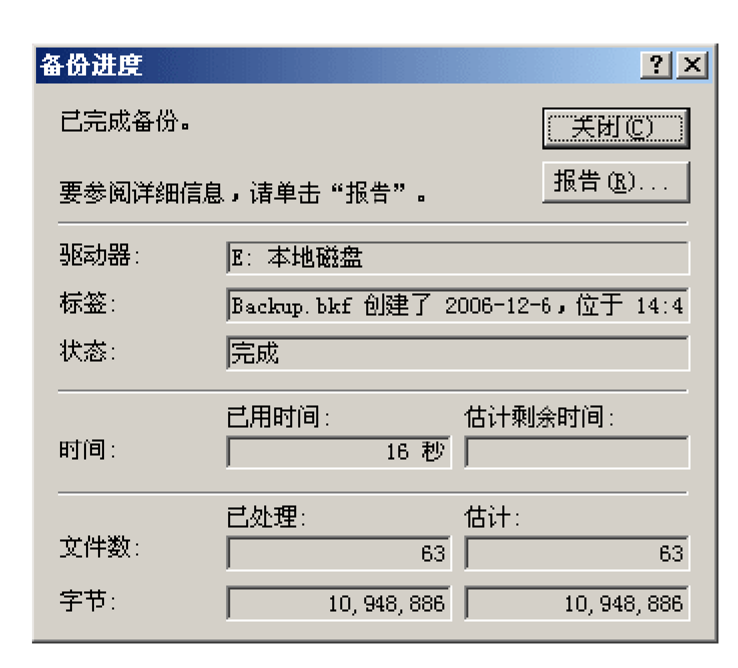


图 9-20　“备份进度”对话框

（5）选择“还原和管理媒体”选项卡，可以对备份文件进行还原，出现如图 9-21 所示。

（6）首先在窗口左边选择需要还原的文件夹，然后在“将文件还原到”下拉列表框中选择还原的目的位置，最后单击“开始还原”按钮，系统还原完成时出现还原结果提示框，如图 9-22 所示。



图 9-21　还原和管理媒体

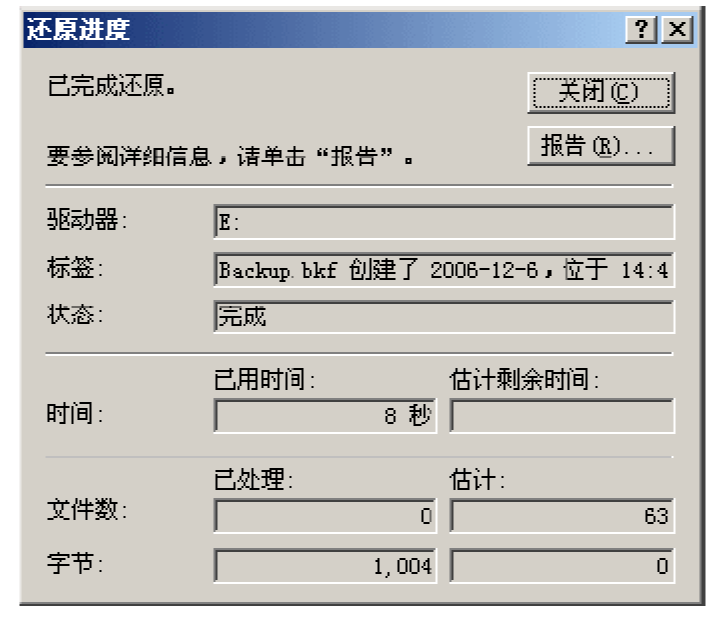


图 9-22　“还原进度”对话框

（7）除了上述讲到的功能以外，还有一些其他的功能，还需要读者多实践操作，达到熟练掌握的目的。

5．配置数据库安全性

如果具有存储用于业务系列应用程序的客户、销售、库存或其他类型的关键信息的数据库，请聘请 IT 专业人士来确保这些信息受到良好的保护。 例如，通过只允许授权用户连接至数据库，数据库专家可以使 Microsoft SQL Server 屏蔽掉大多数基于 Internet 的攻击。 他们还可以创建备份系统，以便在数据丢失时进行还原。

9.4　保护网络安全的 7 个步骤

每天花不到 30 分钟的时间，按照安全检查表中的 7 个要点自行操作，不到两个星期就可以大大地增强对病毒、电脑黑客以及其他安全问题的防护能力。 以下介绍如何着手执行这些步骤。

（1）保护台式机和便携机
（2）保证数据安全
（3）安全地使用 Internet
（4）保护网络
（5）保护服务器
（6）保护业务应用程序
（7）从服务器管理台式机或便携机

9.4.1 保护你的台式机和便携机

如果在保护经营业务所用计算机方面只做三件事，确保做这样三件事，即更新软件、防止病毒和设置防火墙。

它们不能完全防止安全威胁和生产率降低，但同时做好这三件事会为构筑强有力的第一道防线。

1. 更新软件

黑客喜欢查找和利用常用软件产品的程序错误和漏洞。这些黑客有的是为了谋利，有的是为了发表看法，也有的仅仅是为了制造麻烦。 他们可能制造的麻烦包括：在网站上公开客户信用卡号码，或者窃取计算机中的密码。 这对于企业的影响可能是致命的。

可以采取的基本措施如下。

Microsoft 或其他公司一旦发现其软件存在漏洞时，通常会发行更新，可在 Internet 上下载。 更新会“修补”程序漏洞或错误，从而防止黑客制造麻烦。 随着时间的推移，软件产品会变得越来越安全。Windows XP Professional Service Pack2（SP2） 在防止黑客、病毒和蠕虫等方面提供了更强的安全设置。这并不意味着发行修补程序后立即下载和安装不重要。

Windows 更新的安装请参考本书第 6 章相关内容。

2. 防止病毒

病毒、蠕虫和特洛伊木马都是在计算机上运行的恶意程序。 某些病毒会删除或更改文件。 某些会消耗计算机资源。某些会允许外部人员访问文件。 病毒的一个最可恶的特性是它们可以进行复制或自我复制。 病毒可以从联系人列表中获取电子邮件地址，并将其自身发送到这些地址。 感染病毒的计算机会将病毒传遍整个公司，并导致严重的停机和数据丢失。 同时，也会通过电子邮件感染客户或用户的计算机。

防止病毒的具体操作可以参考本书第 2 章相关内容。

3. 设置防火墙

如果具有长期宽带连接，计算机网络会不时受到犯罪性黑客的入侵。他们一旦获取有效的计算机地址，就会试图利用软件漏洞或者破解密码以获取对网络的访问权，最终可以访问网络中的各台计算机和所有内容。

防火墙的基本操作可以参考本书第 4 章以及本章相关内容。

9.4.2 保证数据安全

试想一下，当某天早上走进办公室，却发现所有销售记录、客户联系信息和订单历

史记录全部都不见了。需要花费多长时间才能恢复？会造成多少困扰和延误？会造成多少浪费？

数据丢失很可能会发生，不乏这样的例子。发生的原因可能是硬件故障、水灾、火灾、安全问题，或仅仅是意外地删除了重要的文件。不管是什么原因，采取预防措施以降低影响就像是“保险单”，使企业能够迅速地恢复并运转。

保护关键的业务数据有许多种方法，但以下三种是基本方法：

1．备份关键的数据

备份数据就是在其他介质上保存数据的副本。例如，可以将所有重要的文件刻录到一张 CD-ROM 或第二个硬盘上。有两种基本的备份方法：完整备份和增量备份。完整备份会将所选的数据完整地复制到其他介质。增量备份仅备份上次完整备份以来添加或更改的数据。

通过增量备份扩充完整备份通常较快且占用较少的存储空间。可以考虑每周进行一次完整备份，然后每天进行增量备份。但是，如果要在崩溃后恢复数据，则将花费较长的时间，因为首先必须要恢复完整备份，然后才恢复每个增量备份。如果对此感到担忧，则可以采取另一种方案，每晚进行完整备份；只需使备份在下班后自动运行即可。

通过实际将数据恢复到测试位置来经常测试备份是个好主意。这具有以下作用：

（1）确保备份介质和备份数据状况良好；

（2）确定恢复过程中的问题；

（3）可提供一定程度的信心，这在实际发生危机时将十分有用。

2．建立权限

操作系统和服务器都可对由于员工的活动所造成的数据丢失提供保护。通过 Windows XP 和 Windows 2000 以及 Windows Small Business Server 2003、Windows Server 2003 和 Windows 2000 Server，可以根据用户在组织内的角色和职责而为其分配不同级别的权限。不应为所有用户提供“管理员”访问权，这并不是维护安全环境的最佳做法，而是应制定“赋予最低权限”策略，将服务器配置为赋予各个用户仅能使用特定的程序并明确定义用户权限。

3．对敏感数据加密

对数据加密意味着将其转换为一种可伪装数据的格式。加密用于在网络间存储或移动数据时确保其机密性和完整性。仅那些具有工具来对加密文件进行解密的授权用户可以访问这些文件。加密对其他访问控制方法是一种补充，且对容易被盗的计算机（例如便携式计算机）上的数据或网络上共享的文件提供多一层保护。Windows XP 和 Windows Small Business Server 2003 支持加密文件系统对文件和文件夹加密。

将这三种方法结合起来，应该可以为大多数企业提供保证数据安全所需的保护级别。

9.4.3　安全地使用 Internet

如果企业没有关于 Internet 使用的策略，则应该制定这样的策略。尽管 Web 是非常有用的工作场所工具，它也可能对工作场所造成严重危害，导致生产效率降低。应设置一些规则以保护企业，以及员工。

Web 页面包含一些通常无害的程序，有时很有用，例如动画和弹出菜单。但有一些

可疑的甚至是恶意的网站，它们具有自己的日程，有时会造成危害。 当在网上冲浪时，站点操作员可在 Internet 上识别计算机、识别所访问的网页、使用 cookies 为设置配置文件并在计算机上安装间谍软件，而毫无察觉。 破坏性的蠕虫病毒也可能通过 Web 浏览器进入系统。

除了外部发起的恶意活动，内部员工工作时间在公司计算机上进行非法或不允许的 Web 活动也会使企业易于受到攻击。

当建立公司范围的 Internet 使用策略时，应解决以下问题：

（1）是否允许员工因公和因私浏览 Web；

（2）员工何时可以因私使用 Web（午餐时间、下班后等）；

（3）公司是否监控及如何监控 Web 使用，以及员工可具有怎样的隐私级别；

（4）不允许的 Web 活动。 详细说明不允许的行为。 在许多公司中，不允许的行为包括：

- 下载攻击性的内容
- 恫吓或暴力行为
- 非法活动
- 商业广告（与业务无关）

应向员工提供两份策略：一份由其保存，另一份由其签名并返回给员工。

除了制定相关策略，以下建议也可以有助于安全地进行 Web 浏览：

- 仅浏览受信任的网站；
- 不使用工作计算机进行闲置浏览；
- 切勿从服务器浏览网站。 始终应使用客户端计算机或便携机；
- 使用防火墙/路由器。 它使能够过滤 Web 地址并阻挡来自或去往危险站点的 Internet 流量；
- 考虑使用 Web 过滤软件。 Websense 和 Secure Computing 等公司提供了一些可根据各种条件过滤 Internet 使用的软件。

9.4.4 保护网络

人们常常不会往坏处去想，即到处都有人要探听公司事务。 但如果公司具有有线或无线网络，且具有需保密的信息，那么随时保持警惕是有好处的。

有四种基本措施可以有助于降低网络安全风险。

1. 使用防火墙

防火墙可以控制对网络的访问。 它可以阻止 Internet 入侵者探查专用网络中的数据。它还可以控制员工在网络外部可以访问的内容。

有两种基本类型的防火墙：硬件和软件。 它们的工作原理都是检查传入网络的数据，如果其不符合特定的条件则将其丢弃。 硬件防火墙最适合于网络，因为它们可以保护网络中的所有计算机。 它们还可以增加一层防御，因为它们可有效地使外部“看不到”网络计算机。 软件防火墙（例如内置到 Windows XP Professional 的 Windows 防火墙）仅保护运行它们的计算机，且对硬件防火墙提供了很好的防御支持。

2．使用加强密码

大多数小企业使用密码来在计算机、收银机或报警系统上验证身份。 尽管有更先进的验证系统（例如智能卡和指纹或虹膜扫描），密码仍是最常用的，因为它易于使用。 但是密码也容易盗用。 黑客具有自动的工具，可帮助他们在几分钟之内提供简单的密码。 黑客还可以利用圈套使员工泄露密码。

而且由于以下一些原因，密码常常起不到防护作用：

- 敏感文档未进行密码保护，使任何人可以使用未设保护的计算机并登录；
- 密码简单且/或从不更改；
- 密码写在计算机旁边容易看到的地方。

教育职员使其认识到密码的重要性是使密码成为有效的网络安全工具的基础。 员工应像对待办公室钥匙一样对待密码。 也就是说，不要随处放置密码，也不要让别人知道密码。还应该避免使用简单且易于猜到的密码，包括：

- 他们的真名、用户名或公司名；
- 常见的字典词，这使其容易受到“字典攻击”；
- 常见的密码，例如“password”、“letmein”或“1,2,3,4”；
- 广为人知的字母替换，例如将“i” 替换为“!”或将“s”替换为“$”；
- 为人所知的密码。

什么样的密码是“加强”密码？ 它具有以下特征：

- 至少有八位字符长，越长越好；
- 是小写和大写字母、数字和符号的组合；
- 至少每 90 天要进行更改，而且更改时应与先前的密码有较大区别。

3．使用无线安全功能部件

无线网络使用无线电而不是电缆来连接计算机。 这样，处于无线电范围内的任何人理论上都可以在网络上进行侦听或传输数据。 一些易于获取的工具使入侵者可以“察觉到”不安全的网络。 由于无线网络的安全漏洞较高，精于计算机的黑客具有一些工具可帮助他们侵入所有类型的计算机系统。

有一些安全功能内置到 Wi-Fi 产品中，默认情况下制造商通常将其关闭，因为这样使网络更容易设置。 如果使用无线网络，应确保打开这些功能并使用可配置的加密和访问控制功能，这会使网络更安全。

还应该考虑以下事项：

- 将无线访问限制在工作时间或需要使用网络的任何时间（如果访问点允许）；
- 通过将访问点设置为限制网络仅访问受信任的媒体访问控制（MAC）地址，过滤掉偶然的入侵者；
- 如果使用的是较旧的设备，应升级至功能更强大的 Wi-Fi 保护访问（WPA）加密。

4．关闭不需要的网络端口

网络端口启用客户端计算机和服务器之间的通信。为了加强网络安全并阻止未授权的访问，应该关闭未使用或不需要的网络端口，方法是使用专用的防火墙、基于主机的防火墙或“Internet 协议安全”过滤器。 提示：Microsoft 服务器产品使用各种编号的网络端口

和协议来与客户端和服务器系统进行通信。 阻止 Windows Server System 所使用的端口可能会使服务器无法响应合法的客户端请求，这意味着服务器无法正常工作。

9.4.5 保护服务器

如果将服务器视为网络的命令中心，则容易理解保持安全避免攻击为什么是一个关键任务。一旦危及服务器的安全，整个网络都处于危险之中。虽然有些服务器攻击仅仅是骚扰，但是有些可以引起严重损害。要保护企业，请先保护服务器。

如果为小型企业，可能不具有多个服务器。但是无论正在运行的服务器是多还是少，网络都依靠这些服务器。它们为团队进行工作所需的应用程序、Web 页或电子邮件提供服务。它们存储有价值的和/或机密的信息资源。它们为客户提供与联系的方法，可能从这里购买货物或服务。

因此，如果服务器停机，则会降低生产率并损坏客户关系…… 而且，甚至可能受到经济打击。

已经讨论的许可步骤可帮助保护服务器。因此，如果尚未采取以下步骤，请优先执行这些步骤：

步骤 1：保护台式机和便携机

步骤 2：保证数据安全

步骤 3：安全地使用 Internet

步骤 4：保护网络

即使采用了列出的那些安全措施，还可以采取其他措施来保护服务器。

（1）保持服务器在安全的位置

企业必须确保其服务器不易遇到物理灾难。 将这些机器放置在安全的、通风良好的房间，而不要放在走廊或桌子底下，在这些地方人们可能会无意识地踢到机器或将咖啡溅在机器上。 或者对其进行随意的处理。服务器房间应该没有窗户，且只有一个门，可以锁住这个门。服务器机箱也应该被锁，以防止有人动内部组件。 了解哪些员工持有服务器房间的钥匙。 还应该保存服务器的序列号记录，并将其标记为公司信息，以便被盗后可以识别和发现它们。

（2）赋予最低权限

通过 Windows 2000 Server、Windows Server 2003 和 Small Business Server 2003，可以为用户分配不同的权限级别。 不应为所有用户提供“管理员”访问权，这并不是为计算机或服务器维护安全环境的最佳做法，而是应使用服务器来管理客户端计算机。 Windows 服务器可以配置为指定各个用户仅对特定的程序具有访问权，并定义服务器上允许哪种用户权限。 这确保用户不能在对服务器或客户端计算机操作很关键的地方进行更改。 它还可防止用户安装可能引入病毒的软件，或者危及网络的完整性。

（3）了解安全性选项

目前的服务器比以前的服务器安全，但是 Windows 服务器产品中的功能强大的安全性设置仅当正确使用并加强监控时才有效。如果团队中没有 IT 专家且或不具有安全问题方面的专业知识，则应考虑雇用一个外部顾问，与其一起工作以适当地保护服务器。

9.4.6　保护业务应用程序

许多公司使用专业的业务程序用于会计任务、运行销售点系统、跟踪库存以及管理供应链。

这些程序有时称为业务（line-of-business，LOB）应用程序，通常在服务器上运行并与数据库一起操作。这种集成安装有很多优点。多个员工可以使用一个 LOB 程序并可同时访问数据库信息。例如，在管理员创建自定义的财务报告时，销售人员可以使用此程序记录她的销售号。

但也存在安全风险。位于网络服务器上的客户信息、销售情况、损益表和其他重要业务数据易于受入侵者的攻击。并且，可能并不希望所有员工可以访问所有种类的数据。

问题在于创建一种安全计划，既可以保护 LOB 程序数据完整性和隐私性又支持有效的数据访问和协作。下面介绍了计划中应包含的三种措施。

1．实施基本的安全措施

首先应在工作场所建立基本的计算机安全措施，以保护数据库免受不必要的探听者的威胁以及其他威胁。应该实现以下基本的安全措施。

（1）设置防火墙。防火墙可帮助在 Internet 上阻止入侵者访问计算机和业务数据。使用硬件防火墙效果最好，因为它对企业网络中的所有计算机提供保护。使用软件防火墙提供进一步保护也是一个不错的主意。Windows Small Business Server 2003（许多小型企业将其与业务应用程序一起运行）附带了防火墙技术。服务器软件的高级版本包括 Microsoft Internet Security and Acceleration (ISA) Server，一种高级防火墙解决方案。

（2）在所有计算机上安装防病毒软件。在服务器上运行防病毒软件与在客户端计算机上运行防病毒软件同样重要。 应使用不仅检测和禁用病毒，而且可以定期更新以筛选新病毒的程序。

（3）使用加强密码。在工作场所登录到任何计算机和服务器都应输入密码。加强密码由大小写字母、数字和符号组成。确保要求用户定期更改密码。

（4）备份文件。如果发生灾难，且没有在一个单独的存储系统上保存重要文件和信息，则所有重要业务应用程序数据将会丢失。Windows Small Business Server 2003 包含容易使用的备份功能。

（5）更新软件。软件更新通常包括最新的安全功能。Microsoft 产品的更新可以从 Windows Update 和 Microsoft 下载中心获取。

2．管理对信息的访问权

并非所有人都应该具有对工作场所内所有信息的访问权。如果企业运行的是 Windows Server 操作系统，可以允许和限止员工访问文档、电子表格或其他业务文件。 还可以指定是允许用户只能读取文件还是可更改文件。下面介绍了管理访问权的窍门。

（1）创建多组用户，为这些组（而不是为单个用户）分配权限和优先权。这样可以为管理访问权限节省时间。

（2）根据角色（例如销售代表）创建用户组。然后分配一组权限，这些权限与执行为角色确定的任务有关。

（3）将每个角色的访问权限设置为用户进行工作所需的最低级别。例如，如果销售代

表组只需要读取客户档案，则不要给他们共享或删除文件的访问权限。

一些 LOB 应用程序通过设置访问权限执行大部分工作。其中一个例子是 Microsoft Business Solutions CRM，一种跟踪客户销售和支持关系的高级程序（通常与 Microsoft Small Business Server 2003 一起运行），Microsoft CRM 提供时具有八种预先定义的角色（从 CEO 到业务经理到客户销售代表到专业营销人员）。 此程序还预先定义了可以分配权限的一般商业元素，如销售线索、商机、联系人、账户、竞争对手、产品、销售文献、报价、订单、发票和合同。

3．注意数据库

由于特定于业务的程序通常使用数据库存储应用程序数据，请记住要特别注意数据库的安全性。 下面介绍了可以做的一些事情。

（1）安装最新的数据库 Service Pack。 Windows Small Business Server 2003 提供了 Microsoft SQL Server 2000 Desktop Edition (MSDE 2000)。 服务器软件的高级版本提供了更高级的 Microsoft SQL Server 2000。 当这些数据库程序与业务程序一起使用时，确保安装最新的 Service Pack 和更新以提高安全性。 Microsoft 下载中心有最新的服务器应用程序更新。

（2）使用 MBSA 评估服务器的安全性。 Microsoft Baseline Security Analyzer (MBSA) 是一个在某些 Microsoft 产品（包括 SQL Server 和 MSDE 2000）中搜索常见的不安全配置的工具。

（3）使用 Windows 身份验证模式。 无论何时，要连接到 SQL Server，应要求使用 Windows 身份验证模式。 这将通过将连接限制为 Microsoft Windows 用户和域用户账户来防止 SQL Server 安装受到基于 Internet 的攻击。

（4）隔离服务器并定期备份。 物理和逻辑隔离是 SQL Server 安全的基础。 托管数据库的计算机应位于受到物理保护的位置。 定期备份所有数据并在安全的远程位置存储副本。

9.4.7 从服务器管理台式机或便携机

正当认为已经遵循了保护企业资产免受病毒、黑客和盗贼侵害的所有规则时，某位员工有了“更好”的主意。 即使不是更好的主意，它清楚地表明迄今实施的所有精明的安全措施。

它基本保证了适当地保护企业免受外部威胁。 如果开始执行该过程（更新软件和病毒防护以及安装防火墙），已经投入了大量时间、精力和金钱。

不幸的是，缺乏严格的管理程序会在无意中破坏安全投资，改变所作的更改或无意中引起新的风险。用户可能无法获得最近的更新和修补程序，他们可能会下载未经授权的和有潜在危害的软件，用户可能无法觉察到有人对计算机上的数据进行未经授权的访问。

可以采取以下基本措施。

一种解决方法是从服务器管理台式机和便携机。 此方法不但将降低破坏安全措施的风险，而且它还会因提高效率而节省大量的时间和金钱。

（1）正确的安装

从一开始就可以确保在所有 PC 和便携机上安装操作系统和应用程序的正确版本。

它确保符合许可问题的要求以及在组织中保持一致，以便进行文件共享和其他用途。

（2）及时更新

修补程序和错误修复与新版本软件可以从服务器部署到用户的 PC 和便携机上。 这样可了解它已正确和及时地得到处理，不必依靠用户自己记住做这些事情。

（3）特殊配置

对于每个用户使用的操作系统或应用程序，如果组织具有首选设置，则可以从服务器在组织范围内管理、更新和实施这些设置。 另外，可以通过限制用户从 CD-ROM 和其他可移动驱动器中运行程序或从 Internet 下载程序来防止用户安装未授权的程序。

（4）监控

如果 PC 上出现未授权的访问，或在单个机器上存在某种类型的系统故障，则可通过受管 PC/便携机环境下可用的监控功能立即检测到此情况。

如果正在考虑购买企业的第一台服务器或进行第一次服务器升级，则对于 Windows Server 2003 管理功能的改进以及 Windows XP Professional（带 Service Pack 2）中增强的安全功能等方面可值得留意，它们可提供强大的防护来应对来自内部和外部的威胁。

9.5　及时备份数据

数据是重要的企业资产，但也是最脆弱的资产。例如，硬盘崩溃、病毒或自然灾难都可能导致丢失所有客户清单和财务报表。

不幸的是，大多数企业并不重视备份业务数据，直至遭受严重打击才追悔莫及。但已为时晚矣。

可以轻松创建备份文件，以便还原计算机上的重要业务信息，但这需要规划和不懈的努力。 需要做以下准备。

1．确定保存的内容

第一步，要确定哪些数据需要保护。不需要备份任何文字处理、电子表格或其他类型程序。 程序可以通过原始磁盘重新安装。即使是遭受严重的破坏，也可以相对轻松地获取替代磁盘。

应当担心的是企业创建的相关工作。 包括：

（1）包含客户联系人数据和订购记录的数据库以及库存信息；

（2）财务软件数据文件，包括电子表格；

（3）文档，包括重要信件、备忘录、工作产品以及与业务计划相关的所有内容；

（4）电子邮件，尤其是包含重要数据（如，客户查询和联系人信息）的邮件；

（5）网站文件（除非网站由第三方托管）；

（6）任何其他如果丢失将会给企业造成巨大困难的数据。

还应当保存系统配置文件和其他设置文件（如 Internet 书签），但这些文件并不像其他文件一样重要。

请先确定包含需要备份的文件的文件夹列表，然后再继续操作。

2. 使用备份软件

弄清楚需要保存的内容后，应当开始定期备份。如果手动复制重要文件进行备份，则当有大量文件或文件夹时，将会很耗时耗力。

最好使用备份软件。可以选择使用操作系统附带的备份软件包。Windows XP 和 Windows Small Business Server 2003 都附带有用于备份的工具。Microsoft Windows XP Professional 附带的备份工具已随系统安装。（如果使用 Windows XP Home Edition，则需要从安装光盘上安装。）

要设置 Windows 备份，请单击“开始”按钮，依次指向“所有程序”、“附件”、“系统工具”，然后单击“备份”按钮。 单击“下一步”按钮确认打开的屏幕，选择“备份文件和设置”，然后单击“下一步”按钮。

Windows 备份工具将询问要保存哪些文件。 可能不需要选择“这台计算机上的所有信息”，那样会备份所有内容，包括所有程序文件。 如果安装了许多软件，则最后可能获得一个巨大的备份文件，甚至无法保存。

如果所有人都将其重要文件保存在“我的文档”文件夹中，则可以选择“每个人的文档和设置”。否则，应该选择“让我选择要备份的内容”，然后再选择认为重要的文件夹。完成后，单击“下一步”按钮。

Windows Small Business Server 2003 还附带有备份配置向导，可以指定要复制的文件夹（不管是将备份保存在硬盘驱动器上还是磁带驱动器上）以及应该执行备份的频率。 还可以使用此工具手动启动备份。

3. 了解存储选项

备份工具可以创建一个包含所有重要文档的文件，但需要指定保存文件的位置。 默认情况下，文件将保存至软盘，但如果信息量太大，可能需要成打甚至上百个软盘。

还可以选择将备份保存到网络上或计算机中另外一个硬盘驱动器上。只需单击“浏览”按钮，然后选择保存文件的位置即可。为文件指定一个描述性名称，然后单击“下一步”按钮。

如果硬盘发生故障或被病毒感染，这种类型的备份可以提供一些保护，但如果发生火灾或自然灾难，可能会失去整台计算机和全部数据。 因此，应当定期将备份文件复制到 CD、DVD 或外部驱动器上，并保存在办公场所以外的安全位置。

可以从在 Windows 备份中指定的文件夹中找到备份文件。如果该文件少于 640 兆字节，可以使用 CD 刻录机将文件保存到标准的 CD-ROM 上。如果更大，需要使用 DVD。确保刻录机可以写入可记录 DVD。

还可以使用可重复使用的介质，如闪存或外挂硬盘驱动器。检查备份文件的大小以确定需要多少存储空间。

4. 更多备份建议

此处提供了一些在执行备份时可以参考的其他建议：

（1）坚持计划。 请切记，数据的安全取决于最后一次备份。 如果硬盘驱动器崩溃了，但已有一个月未备份数据了，那么将丢失掉一个月的辛勤工作。 这就是为什么定期备份数据如此重要。 可能每晚都要将文件备份至硬盘驱动器或网络服务器。备份工具可以选择备份频率及时间。

（2）非现场存储。尽管每晚都将数据备份到网络或磁带上不失为一个好主意，但仍需

要制定一个计划将文件保存到 CD、DVD 或可移动存储设备上，供非现场传送使用。备份的频率视企业可以承受丢失数据的程度而定。

（3）练习还原数据。最好永远都不要使用备份，但最好还是了解还原数据并不比备份数据轻松。如果使用 Windows Small Business Server 2003，则可按照其步骤将整个服务器上的全部内容还原为单个文件。Windows 备份也支持使用备份文件执行还原。应当在使用前测试备份步骤。请使用只安装了操作系统，但未接入网络的计算机。如果测试现有网络上的备份，则可能意外以旧数据覆盖新文件，或错误识别潜在问题。

备份是灾难和系统故障的有力保障，但前提是必须抽出时间定期备份系统。

9.6 保护敏感文档

在计算机诞生前，要想找到重要的公司报告和记录，必须离开自己的座位，然后在锁着的文件柜中大找特找。

但是，今天的数字化工作场所已经大大简化了文档的使用过程。坐在 PC 前面的员工或者某个聪明的外部人员，只要单击几下鼠标就能查找和查看几乎所有公司文档。

企业所有者对此异常关注。未经授权地查看和分发机密客户数据、财务记录、员工信息、产品规格以及其他敏感文档可能给公司带来灾难。泄露机密信息可能导致公司的利润损失、威胁到公司的竞争实力、无法公正地做出采购和聘用决策、降低客户信任度等问题。例如，如果有人将工资单报告传播出去，可能就会引起员工的不满情绪。

如何防止其他人未经授权地查看敏感文档？下面介绍几种对机密文档进行保密的策略。

1. 保护文档的几种简单方法

以下几种简单方法和现成的技术工具对保护文档的安全大有帮助。

（1）销毁硬拷贝。如果在开会期间打印出机密文档以便大家传阅，请在会后将它们集中收集起来，然后亲自或要求与会者将它们销毁。

（2）标记文档。有时，员工可能不知道文档中包含机密信息，因此没有采取预防措施。如果知道，他们肯定会采取措施。因此，请告诉作者在页眉或页脚处标明“机密”字样。他们也可以在文档上加个机密水印。在 Word 2003 中，从“格式”菜单中选择“背景”，然后选择“水印”。在对话框中选择“文字水印”，然后从下拉列表中选择“保密”。

（3）使用密码保护。通过要求要打开文档的用户知道并且输入创建并与他们共享的密码，可以限制查看文档的用户。使用 Microsoft Office 2003 创建的文档、电子表格和演示文稿全都具有此功能。只需打开文件，从“工具”菜单中选择“选项”，然后单击“安全性”选项卡。可以设置打开和修改文档的密码。虽然黑客有发现密码的工具，但是密码通常可以增加查看文档的难度。

（4）安装防火墙。安装防火墙有许多理由，保护重要文档无疑是其中比较重要的一个。防火墙可以阻止 Internet 入侵者访问计算机文件和查看信息。Windows XP Professional 附带一个很容易设置的软件防火墙。

（5）锁门。为了防止其他人进入办公室，搬走计算机并且将硬盘上的所有文档顺手牵

羊，请不要将计算机留在无人看管的区域并且确保下班后锁好办公室门。如果还有服务器，请将它放在全天候上锁的特殊区域内。

2．高级文档保护

由于许多保护敏感文档的解决方案都非常复杂，因此需要技术顾问的帮助。但是，如果文档安全是首要问题，需要仔细考虑以下策略。

（1）加密文档文件

如果公司的计算机被盗，加密可以保护文档的安全。对于经常携带便携式计算机出差的商业人士来说，加密是一种非常可靠的技术。数据加密之后，只有那些拥有安装在他们计算机上的必要“密钥”的用户才能访问，其他人无法访问。

Windows XP Professional 附带加密文件系统（EFS），可以利用它来加密单个文件以及整个文件夹的内容。利用 EFS，只有加密文档的用户才能打开文档并且对其进行处理。 不过，内置的数据恢复支持允许在员工离职后或文件加密密钥丢失后恢复员工加密的数据。

虽然加密听起来技术性很强，但是并不需要外部顾问来教如何使用它。EFS 的默认配置使用户不必花费过多的精力就能开始加密文件并且创建所需的全部密钥。

（2）分配文件权限

如果企业使用服务器，可以通过分配权限来限制查看或更改文档的用户。 基本上可以按照所有者的要求授予或拒绝用户对文档（或任何计算机资源）的访问权限。

访问权限适用于个人以及用户组。通用权限允许用户查看或读取一个文件或一个文件夹中的所有文件，以及更改或写入一个文件或一个文件夹中的所有文件。Windows Small Businesses Server 2003 以及其他 Windows Server 系统使可以通过“访问控制列表”来使用权限。

（3）使用信息权限管理

对于直接与 Microsoft Office Professional 2003 版的 Word、Excel、PowerPoint 和 Outlook 集成的文档保护系统，可以考虑使用 Microsoft 公司开发的信息权限管理 (IRM) 技术。

利用 IRM，可以设置不同级别的文件权限并且更改特定用户和用户组的级别。也可以：

- 限制文件打印，以便减少生成的硬拷贝数
- 限制文件打开的时间范围
- 阻止未经授权的收件人打开转发的文件

此外，即使在电子邮件消息和附件发送出去之后，也可以利用 IRM 来控制它们。 它可以阻止其他人复制、转发或打印电子邮件消息。

IRM 要求公司服务器必须运行 Windows Server 2003。

对于大多数情况，只要严加防范并且利用常识就能很好地保护敏感文档。 但是，企业因泄露报告、报表以及其他机密文档而遭受的损失越大，需要在文档保护解决方案上的投资也就越大。 而在数字化高度发展的今天，这并不表示需要再给文件柜加上一把锁。

9.7 日志分析

通常情况下，计算机系统和网络设备都为我们提供了记录操作日志的功能，也就是说，

可以根据需要，对各种操作记录日志信息，因为这是由操作系统来完成的，不管是正常操作还是攻击操作，都会被记录下来，然后通过定期或者不定期的日志分析检查，就可以发现计算机系统和网络设备是否受到攻击以及攻击的相关信息。

1．日志监测和分析的重要性

日志数据可以是有价值的信息宝库，也可以是毫无价值的数据泥潭。要保护和提高你的网络安全，由各种操作系统、应用程序、设备和安全产品的日志数据能够帮助你提前发现和避开灾难，并且找到安全事件的根本原因。

当然，日志数据对于实现网络安全的价值有多大取决于两个因素：第一，你的系统和设备必须进行合适的设置以便记录你需要的数据。第二，你必须有合适的工具、培训和可用的资源来分析收集到的数据。

（1）你不能分析你没有的东西

在你能够分析日志数据之前，你显然要收集数据。更重要的是，记录数据的程序或者设备要设置为收集你需要的数据。例如，微软的 Windows 操作系统在“Event Viewer Security”（安全事件观察器）中能够检查到各种活动和日志信息。然而，在 Windows 2000 和 XP 中，安全检查功能并不是默认启用的，Windows Server 2003 默认的安全检查设置也许不能满足你的需求。

对于 Windows 中的安全检查事件，你可以选择记录成功的尝试，或者记录失败的尝试。如果你仅选择记录失败的访问文件和文件夹的数据，记录的数据就不会显示这个文件是什么时候被成功破解的。如果你仅记录成功地访问一个用户账号的尝试，记录的数据就不会向你显示一个黑客 50 次没有猜对那个账号的用户名和密码。

无论你是在使用 Windows 操作系统还是任何其他的设备和程序，你必须花费一些时间和努力事先了解你拥有的安全日志功能，并且为你的需要恰当地设置好日志选项。虽然简单地把一切都记录下来似乎是合乎逻辑的，但是，监测和记录安全事件会给处理器增加工作负担并且要使用内存和硬盘的空间。你需要了解可用的日志选项，在记录一切和全不记录之间选择最佳的平衡点，以便记录对你有价值的数据。

（2）信息过载

一旦你收集完日志数据，这个挑战就是如何有效地利用这些数据。位于新泽西州 Edison 的 netForensics 公司安全战略家 Anton Chuvakin 指出：“一旦技术合适和收集完日志，就需要实施一个监测程序并且评估行动中的陷阱和可能的升级”。

网络和安全管理员经常花费时间建立日志数据收集，但是，他们没有处理这些数据或者没有现成的资源来监测和分析那些数据。因为没有人监测这些日志数据，有关网络侦察或者潜在的攻击的信息也许会被忽略而失去时效。

当安全事件发生时，查看日志数据也许可以确定事件发生的时间。但是，在很多情况下，需要查看的数据量太大，人们没有经过技术培训或者不会查看这些数据，有日志数据也没有意义了。

现在，有安全事件管理（SEM）应用软件等一些工具专门用于监测安全事件并且使用某些逻辑或者过滤器帮助管理员获取有意义的数据。然而，这些工具仍需要设置和恰当地使用才能有效率。人们要对过滤的数据有所了解并且采取措施。

收集堆积如山的事件日志数据，如果没有经过培训的人员和资源对这些日志数据进行

监测和分析，就如同没有收集任何数据一样毫无用处。下面我们将提供一些技巧，帮助你了解这些日志数据的意义，并且使用这些数据保护你的网络和增强网络的安全。

2．如何有效使用日志数据

日志数据在管理计算机或者网络方面是一种有价值的和实用的工具。事先监测日志数据以寻找可疑的活动迹象的能力或者在发生安全事件时分析日志数据是非常有价值的。

第一步是确保你的系统和设备进行了正确的配置，以便检查和记录事件。假设日志数据已经被捕捉和存储，你需要一个有效的工作流程来检查和分析这些数据。下面的一些建议可以向你提供一些指南并且确保你最有效和最充分地使用你的日志数据。

（1）有规律地检查日志数据

虽然日志数据在安全事件发生时用作法院的证据是非常有效的，但是，如果有规律地分析这些日志数据，这种安全事件也许根本就不会发生。

应该建立一个工作流程，确定多长时间检查和分析一次收集到的日志数据。定期分析由整个网络中的各种应用程序和设备收集到的海量日志数据有助于找出和诊断故障，还可能发现正在进行中的攻击。

（2）以开放的眼光查看日志信息

在分析日志数据时常见的错误是要具体找出已知的事件或者日志项。然而，日志数据中多数有价值的内容似乎存在于表面上很好或者正常的日志项目中。通过以开放的眼光检查这些日志项目，你也许会找到可疑的活动迹象。如果你仅仅查看错误信息，这种迹象很可能会漏掉。

如果把日志审查的重点放在查找已知的恶意活动方面，任何新出现的威胁或者对客户的攻击都会由于失查而漏掉。

（3）通过一个透镜查看数据

整个网络中的设备和应用程序将收集日志数据。遗憾的是没有一种通用的格式或者方法来记录和显示事件的信息。

为了进行准确的比对，某种形式的转化便产生了，也就是对日志数据实施“正常化”。一旦数据压缩为通用的组件，就很容易把这个网络作为一个整体进行分析，而不是作为一个单独的日志项目进行分析。这样就可以更好地根据轻重缓急对发现的问题进行处理或者做出反应。

习题

1．网络安全实施原则是什么？
2．网络安全措施包括的 15 项内容是什么？
3．保护网络安全的 7 个步骤是什么？
4．怎样保护敏感文件？
5．怎样通过日志分析检查网络安全？